Chapter 4
The Algebra–Geometry Dictionary

In this chapter, we will explore the correspondence between ideals and varieties. In §§1 and 2, we will prove the Nullstellensatz, a celebrated theorem which identifies exactly which ideals correspond to varieties. This will allow us to construct a "dictionary" between geometry and algebra, whereby any statement about varieties can be translated into a statement about ideals (and conversely). We will pursue this theme in §§3 and 4, where we will define a number of natural algebraic operations on ideals and study their geometric analogues. In keeping with the computational emphasis of the book, we will develop algorithms to carry out the algebraic operations. In §§5 and 6, we will study the more important algebraic and geometric concepts arising out of the Hilbert Basis Theorem: notably the possibility of decomposing a variety into a union of simpler varieties and the corresponding algebraic notion of writing an ideal as an intersection of simpler ideals. In §7, we will prove the Closure Theorem from Chapter 3 using the tools developed in this chapter.

§1 Hilbert's Nullstellensatz

In Chapter 1, we saw that a variety $V \subseteq k^n$ can be studied by passing to the ideal

$$\mathbf{I}(V) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in V\}$$

of all polynomials vanishing on V. Hence, we have a map

$$\begin{array}{ccc} \text{affine varieties} & & \text{ideals} \\ V & \longrightarrow & \mathbf{I}(V). \end{array}$$

Conversely, given an ideal $I \subseteq k[x_1, \ldots, x_n]$, we can define the set

$$\mathbf{V}(I) = \{a \in k^n \mid f(a) = 0 \text{ for all } f \in I\}.$$

D.A. Cox et al., *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, DOI 10.1007/978-3-319-16721-3_4

The Hilbert Basis Theorem assures us that $\mathbf{V}(I)$ is actually an affine variety, for it tells us that there exists a finite set of polynomials $f_1, \ldots, f_s \in I$ such that $I = \langle f_1, \ldots, f_s\rangle$, and we proved in Proposition 9 of Chapter 2, §5 that $\mathbf{V}(I)$ is the set of common roots of these polynomials. Thus, we have a map

$$\begin{array}{ccc} \text{ideals} & & \text{affine varieties} \\ I & \longrightarrow & \mathbf{V}(I). \end{array}$$

These two maps give us a correspondence between ideals and varieties. In this chapter, we will explore the nature of this correspondence.

The first thing to note is that this correspondence (more precisely, the map $\mathbf{V}$) is not one-to-one: different ideals can give the same variety. For example, $\langle x\rangle$ and $\langle x^2\rangle$ are different ideals in $k[x]$ which have the same variety $\mathbf{V}(x) = \mathbf{V}(x^2) = \{0\}$. More serious problems can arise if the field k is not algebraically closed. For example, consider the three polynomials $1,\ 1 + x^2$, and $1 + x^2 + x^4$ in $\mathbb{R}[x]$. These generate different ideals

$$I_1 = \langle 1\rangle = \mathbb{R}[x], \quad I_2 = \langle 1 + x^2\rangle, \quad I_3 = \langle 1 + x^2 + x^4\rangle,$$

but each polynomial has no real roots, so that the corresponding varieties are all empty:

$$\mathbf{V}(I_1) = \mathbf{V}(I_2) = \mathbf{V}(I_3) = \emptyset.$$

Examples of polynomials in two variables without real roots include $1 + x^2 + y^2$ and $1 + x^2 + y^4$. These give different ideals in $\mathbb{R}[x, y]$ which correspond to the empty variety.

Does this problem of having different ideals represent the empty variety go away if the field k is algebraically closed? It does in the one-variable case when the ring is $k[x]$. To see this, recall from §5 of Chapter 1 that any ideal I in $k[x]$ can be generated by a single polynomial because $k[x]$ is a principal ideal domain. So we can write $I = \langle f\rangle$ for some polynomial $f \in k[x]$. Then $\mathbf{V}(I)$ is the set of roots of f; i.e., the set of $a \in k$ such that $f(a) = 0$. But since k is algebraically closed, every nonconstant polynomial in $k[x]$ has a root. Hence, the only way that we could have $\mathbf{V}(I) = \emptyset$ would be to have f be a nonzero constant. In this case, $1/f \in k$. Thus, $1 = (1/f) \cdot f \in I$, which means that $g = g \cdot 1 \in I$ for all $g \in k[x]$. This shows that $I = k[x]$ is the only ideal of $k[x]$ that represents the empty variety when k is algebraically closed.

A wonderful thing now happens: the same property holds when there is more than one variable. In any polynomial ring, algebraic closure is enough to guarantee that the only ideal which represents the empty variety is the entire polynomial ring itself. This is the *Weak Nullstellensatz*, which is the basis of (and is equivalent to) one of the most celebrated mathematical results of the late nineteenth century, Hilbert's Nullstellensatz. Such is its impact that, even today, one customarily uses the original German name *Nullstellensatz*: a word formed, in typical German fashion, from three simpler words: Null (= Zero), Stellen (= Places), Satz (= Theorem).

Theorem 1 (The Weak Nullstellensatz). *Let k be an algebraically closed field and let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal satisfying $\mathbf{V}(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$.*

Proof. Our proof is inspired by GLEBSKY (2012). We will prove the theorem in contrapositive form:

$$I \subsetneq k[x_1, \ldots, x_n] \Longrightarrow \mathbf{V}(I) \neq \emptyset.$$

We will make frequent use of the standard equivalence $I = k[x_1, \ldots, x_n] \Leftrightarrow 1 \in I$. This is part (a) of Exercise 16 from Chapter 1, §4.

Given $a \in k$ and $f \in k[x_1, \ldots, x_n]$, let $\bar{f} = f(x_1, \ldots, x_{n-1}, a) \in k[x_1, \ldots, x_{n-1}]$. Similar to Exercise 2 of Chapter 3, §5 and Exercise 15 of Chapter 3, §6, the set

$$I_{x_n=a} = \{\bar{f} \mid f \in I\}$$

is an ideal of $k[x_1, \ldots, x_{n-1}]$. The key step in the proof is the following claim.

Claim. If k is algebraically closed and $I \subsetneq k[x_1, \ldots, x_n]$ is a proper ideal, then there is $a \in k$ such that $I_{x_n=a} \subsetneq k[x_1, \ldots, x_{n-1}]$.

Once we prove the claim, an easy induction gives elements $a_1, \ldots, a_n \in k$ such that $I_{x_n=a_n, \ldots, x_1=a_1} \subsetneq k$. But the only ideals of k are $\{0\}$ and k (Exercise 3), so that $I_{x_n=a_n, \ldots, x_1=a_1} = \{0\}$. This implies $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. We conclude that $\mathbf{V}(I) \neq \emptyset$, and the theorem will follow.

To prove the claim, there are two cases, depending on the size of $I \cap k[x_n]$.

Case 1. $I \cap k[x_n] \neq \{0\}$. Let $f \in I \cap k[x_n]$ be nonzero, and note that f is nonconstant, since otherwise $1 \in I \cap k[x_n] \subseteq I$, contradicting $I \neq k[x_1, \ldots, x_n]$.

Since k is algebraically closed, $f = c \prod_{i=1}^{r} (x_n - b_i)^{m_i}$ where $c, b_1, \ldots, b_r \in k$ and $c \neq 0$. Suppose that $I_{x_n=b_i} = k[x_1, \ldots, x_{n-1}]$ for all i. Then for all i there is $B_i \in I$ with $B_i(x_1, \ldots, x_{n-1}, b_i) = 1$. This implies that

$$1 = B_i(x_1, \ldots, x_{n-1}, b_i) = B_i(x_1, \ldots, x_{n-1}, x_n - (x_n - b_i)) = B_i + A_i(x_n - b_i)$$

for some $A_i \in k[x_1, \ldots, x_n]$. Since this holds for $i = 1, \ldots, r$, we obtain

$$1 = \prod_{i=1}^{r} (A_i(x_n - b_i) + B_i)^{m_i} = A \prod_{i=1}^{r} (x_n - b_i)^{m_i} + B,$$

where $A = \prod_{i=1}^{r} A_i^{m_i}$ and $B \in I$. This and $\prod_{i=1}^{r} (x_n - b_i)^{m_i} = c^{-1} f \in I$ imply that $1 \in I$, which contradicts $I \neq k[x_1, \ldots, x_n]$. Thus $I_{x_n=b_i} \neq k[x_1, \ldots, x_{n-1}]$ for some i. This b_i is the desired a.

Case 2. $I \cap k[x_n] = \{0\}$. Let $\{g_1, \ldots, g_t\}$ be a Gröbner basis of I for lex order with $x_1 > \cdots > x_n$ and write

$$g_i = c_i(x_n) x^{\alpha_i} + \text{terms} < x^{\alpha_i}, \tag{1}$$

where $c_i(x_n) \in k[x_n]$ is nonzero and x^{α_i} is a monomial in $x_1, \ldots, x_{n-1}$.

Now pick $a \in k$ such that $c_i(a) \neq 0$ for all i. This is possible since algebraically closed fields are infinite by Exercise 4. It is easy to see that the polynomials

$$\bar{g}_i = g_i(x_1, \ldots, x_{n-1}, a)$$

form a basis of $I_{x_n=a}$ (Exercise 5). Substituting $x_n = a$ into equation (1), one easily sees that $\mathrm{LT}(\bar{g}_i) = c_i(a)x^{\alpha_i}$ since $c_i(a) \neq 0$. Also note that $x^{\alpha_i} \neq 1$, since otherwise $g_i = c_i \in I \cap k[x_n] = \{0\}$, yet $c_i \neq 0$. This shows that $\mathrm{LT}(\bar{g}_i)$ is nonconstant for all i.

We claim that the $\bar{g}_i$ form a Gröbner basis of $I_{x_n=a}$. Assuming the claim, it follows that $1 \notin I_{x_n=a}$ since no $\mathrm{LT}(\bar{g}_i)$ can divide 1. Thus $I_{x_n=a} \neq k[x_1, \ldots, x_{n-1}]$, which is what we want to show.

To prove the claim, take $g_i, g_j \in G$ and consider the polynomial

$$S = c_j(x_n)\,\frac{x^\gamma}{x^{\alpha_i}}\,g_i - c_i(x_n)\,\frac{x^\gamma}{x^{\alpha_j}}\,g_j,$$

where $x^\gamma = \mathrm{lcm}(x^{\alpha_i}, x^{\alpha_j})$. By construction, $x^\gamma > \mathrm{LT}(S)$ (be sure you understand this). Since $S \in I$, it has a standard representation $S = \sum_{l=1}^t A_l g_l$. Then evaluating at $x_n = a$ gives

$$c_j(a)\frac{x^\gamma}{x^{\alpha_i}}\bar{g}_i - c_i(a)\frac{x^\gamma}{x^{\alpha_j}}\bar{g}_j = \overline{S} = \textstyle\sum_{l=1}^t \bar{A}_l \bar{g}_l.$$

Since $\mathrm{LT}(\bar{g}_i) = c_i(a)x^{\alpha_i}$, we see that $\overline{S}$ is the S-polynomial $S(\bar{g}_i, \bar{g}_j)$ up to the nonzero constant $c_i(a)c_j(a)$. Then

$$x^\gamma > \mathrm{LT}(S) \geq \mathrm{LT}(A_l g_l), \quad A_l g_l \neq 0$$

implies that

$$x^\gamma > \mathrm{LT}(\bar{A}_l \bar{g}_l), \quad \bar{A}_l \bar{g}_l \neq 0$$

(Exercise 6). Since $x^\gamma = \mathrm{lcm}(\mathrm{LM}(\bar{g}_i), \mathrm{LM}(\bar{g}_j))$, it follows that $S(\bar{g}_i, \bar{g}_j)$ has an lcm representation for all i, j and hence is a Gröbner basis by Theorem 6 of Chapter 2, §9. This proves the claim and completes the proof of the theorem. □

In the special case when $k = \mathbb{C}$, the Weak Nullstellensatz may be thought of as the "Fundamental Theorem of Algebra for multivariable polynomials"—every system of polynomials that generates an ideal strictly smaller than $\mathbb{C}[x_1, \ldots, x_n]$ has a common zero in $\mathbb{C}^n$.

The Weak Nullstellensatz also allows us to solve the *consistency problem* from §2 of Chapter 1. Recall that this problem asks whether a system

$$\begin{aligned} f_1 &= 0, \\ f_2 &= 0, \\ &\vdots \\ f_s &= 0 \end{aligned}$$

of polynomial equations has a common solution in $\mathbb{C}^n$. The polynomials fail to have a common solution if and only if $\mathbf{V}(f_1,\ldots,f_s)=\emptyset$. By the Weak Nullstellensatz, the latter holds if and only if $1\in\langle f_1,\ldots,f_s\rangle$. Thus, to solve the consistency problem, we need to be able to determine whether 1 belongs to an ideal. This is made easy by the observation that for any monomial ordering, $\{1\}$ *is the only reduced Gröbner basis of the ideal* $\langle 1\rangle = k[x_1,\ldots,x_n]$.

To see this, let $\{g_1,\ldots,g_t\}$ be a Gröbner basis of $I=\langle 1\rangle$. Thus, $1\in\langle \mathrm{LT}(I)\rangle = \langle \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)\rangle$, and then Lemma 2 of Chapter 2, §4 implies that 1 is divisible by some $\mathrm{LT}(g_i)$, say $\mathrm{LT}(g_1)$. This forces $\mathrm{LT}(g_1)$ to be constant. Then every other $\mathrm{LT}(g_i)$ is a multiple of that constant, so that $g_2,\ldots,g_t$ can be removed from the Gröbner basis by Lemma 3 of Chapter 2, §7. Finally, since $\mathrm{LT}(g_1)$ is constant, g_1 itself is constant since every nonconstant monomial is >1 (see Corollary 6 of Chapter 2, §4). We can multiply by an appropriate constant to make $g_1=1$. Our reduced Gröbner basis is thus $\{1\}$.

To summarize, we have the following **consistency algorithm**: if we have polynomials $f_1,\ldots,f_s\in\mathbb{C}[x_1,\ldots,x_n]$, we compute a reduced Gröbner basis of the ideal they generate with respect to any ordering. If this basis is $\{1\}$, the polynomials have no common zero in $\mathbb{C}^n$; if the basis is not $\{1\}$, they must have a common zero. Note that this algorithm works over any algebraically closed field.

If we are working over a field k which is not algebraically closed, then the consistency algorithm still works in one direction: if $\{1\}$ is a reduced Gröbner basis of $\langle f_1,\ldots,f_s\rangle$, then the equations $f_1=\cdots=f_s=0$ have no common solution. The converse is not true, as shown by the examples preceding the statement of the Weak Nullstellensatz.

Inspired by the Weak Nullstellensatz, one might hope that the correspondence between ideals and varieties is one-to-one provided only that one restricts to algebraically closed fields. Unfortunately, our earlier example $\mathbf{V}(x)=\mathbf{V}(x^2)=\{0\}$ works over *any* field. Similarly, the ideals $\langle x^2,y\rangle$ and $\langle x,y\rangle$ (and, for that matter, $\langle x^n,y^m\rangle$ where n and m are integers greater than one) are different but define the same variety: namely, the single point $\{(0,0)\}\subseteq k^2$. These examples illustrate a basic reason why different ideals can define the same variety (equivalently, that the map $\mathbf{V}$ can fail to be one-to-one): namely, a power of a polynomial vanishes on the same set as the original polynomial. The Hilbert Nullstellensatz states that over an algebraically closed field, this is the *only* reason that different ideals can give the same variety: if a polynomial f vanishes at all points of some variety $\mathbf{V}(I)$, then some power of f must belong to I.

Theorem 2 (Hilbert's Nullstellensatz). *Let k be an algebraically closed field. If $f,f_1,\ldots,f_s\in k[x_1,\ldots,x_n]$, then $f\in\mathbf{I}(\mathbf{V}(f_1,\ldots,f_s))$ if and only if*

$$f^m\in\langle f_1,\ldots,f_s\rangle$$

for some integer $m\geq 1$.

Proof. Given a nonzero polynomial f which vanishes at every common zero of the polynomials $f_1,\ldots,f_s$, we must show that there exists an integer $m\geq 1$ and polynomials $A_1, \ldots, A_s$ such that

$$f^m = \sum_{i=1}^{s} A_i f_i.$$

The most direct proof is based on an ingenious trick. Consider the ideal

$$\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq k[x_1, \ldots, x_n, y],$$

where $f, f_1, \ldots, f_s$ are as above. We claim that

$$\mathbf{V}(\tilde{I}) = \emptyset.$$

To see this, let $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$. Either

- $(a_1, \ldots, a_n)$ is a common zero of $f_1, \ldots, f_s$, or
- $(a_1, \ldots, a_n)$ is not a common zero of $f_1, \ldots, f_s$.

In the first case $f(a_1, \ldots, a_n) = 0$ since f vanishes at any common zero of $f_1, \ldots, f_s$. Thus, the polynomial $1 - yf$ takes the value $1 - a_{n+1}f(a_1, \ldots, a_n) = 1 \neq 0$ at the point $(a_1, \ldots, a_n, a_{n+1})$. In particular, $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$. In the second case, for some $i, 1 \leq i \leq s$, we must have $f_i(a_1, \ldots, a_n) = 0$. Thinking of f_i as a function of $n + 1$ variables which does not depend on the last variable, we have $f_i(a_1, \ldots, a_n, a_{n+1}) \neq 0$. In particular, we again conclude that $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$. Since $(a_1, \ldots, a_n, a_{n+1}) \in k^{n+1}$ was arbitrary, we obtain $\mathbf{V}(\tilde{I}) = \emptyset$, as claimed.

Now apply the Weak Nullstellensatz to conclude that $1 \in \tilde{I}$. Hence

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf) \tag{2}$$

for some polynomials $p_i, q \in k[x_1, \ldots, x_n, y]$. Now set $y = 1/f(x_1, \ldots, x_n)$. Then relation (2) above implies that

$$1 = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n, 1/f) f_i. \tag{3}$$

Multiply both sides of this equation by a power f^m, where m is chosen sufficiently large to clear all the denominators. This yields

$$f^m = \sum_{i=1}^{s} A_i f_i, \tag{4}$$

for some polynomials $A_i \in k[x_1, \ldots, x_n]$, which is what we had to show. $\square$

EXERCISES FOR §1

1. Recall that $\mathbf{V}(y - x^2, z - x^3)$ is the twisted cubic in $\mathbb{R}^3$.
   a. Show that $\mathbf{V}((y - x^2)^2 + (z - x^3)^2)$ is also the twisted cubic.
   b. Show that any variety $\mathbf{V}(I) \subseteq \mathbb{R}^n$, $I \subseteq \mathbb{R}[x_1, \ldots, x_n]$, can be defined by a single equation (and hence by a principal ideal).
2. Let $J = \langle x^2 + y^2 - 1, y - 1\rangle$. Find $f \in \mathbf{I}(\mathbf{V}(J))$ such that $f \notin J$.
3. Prove that $\{0\}$ and k are the only ideals of a field k.
4. Prove that an algebraically closed field k must be infinite. Hint: Given n elements $a_1, \ldots, a_n$ of a field k, can you write down a nonconstant polynomial $f \in k[x]$ with the property that $f(a_i) = 1$ for all i?
5. In the proof of Theorem 1, prove that $I_{x_n=a} = \langle \bar{g}_1, \ldots, \bar{g}_t\rangle$.
6. In the proof of Theorem 1, let x^δ be a monomial in $x_1, \ldots, x_{n-1}$ satisfying $x^\delta > \mathrm{LT}(f)$ for some $f \in k[x_1, \ldots, x_n]$. Prove that $x^\delta > \mathrm{LT}(\bar{f})$, where $\bar{f} = f(x_1, \ldots, x_{n-1}, a)$.
7. In deducing Hilbert's Nullstellensatz from the Weak Nullstellensatz, we made the substitution $y = 1/f(x_1, \ldots, x_n)$ to deduce relations (3) and (4) from (2). Justify this rigorously. Hint: In what set is $1/f$ contained?
8. The purpose of this exercise is to show that if k is any field that is not algebraically closed, then *any* variety $V \subseteq k^n$ can be defined by a *single* equation.
   a. If $g = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ is a polynomial of degree n in x, define the *homogenization* g^h of g with respect to some variable y to be the polynomial $g^h = a_0x^n + a_1x^{n-1}y + \cdots + a_{n-1}xy^{n-1} + a_ny^n$. Show that g has a root in k if and only if there is $(a, b) \in k^2$ such that $(a, b) \neq (0, 0)$ and $g^h(a, b) = 0$. Hint: Show that $g^h(a, b) = b^n g^h(a/b, 1)$ when $b \neq 0$.
   b. If k is not algebraically closed, show that there exists $f \in k[x, y]$ such that the variety defined by $f = 0$ consists of just the origin $(0, 0) \in k^2$. Hint: Choose a polynomial in $k[x]$ with no root in k and consider its homogenization.
   c. If k is not algebraically closed, show that for each integer $l > 0$ there exists $f \in k[x_1, \ldots, x_l]$ such that the only solution of $f = 0$ is the origin $(0, \ldots, 0) \in k^l$. Hint: Use induction on l and part (b) above.
   d. If $W = \mathbf{V}(g_1, \ldots, g_s)$ is any variety in k^n, where k is not algebraically closed, then show that W can be defined by a single equation. Hint: Consider the polynomial $f(g_1, \ldots, g_s)$ where f is as in part (c).
9. Let k be an arbitrary field and let S be the subset of all polynomials in $k[x_1, \ldots, x_n]$ that have no zeros in k^n. If I is any ideal in $k[x_1, \ldots, x_n]$ such that $I \cap S = \emptyset$, show that $\mathbf{V}(I) \neq \emptyset$. Hint: When k is not algebraically closed, use the previous exercise.
10. In Exercise 1, we encountered two ideals in $\mathbb{R}[x, y]$ that give the same nonempty variety. Show that one of these ideals is contained in the other. Can you find two ideals in $\mathbb{R}[x, y]$, neither contained in the other, which give the same nonempty variety? Can you do the same for $\mathbb{R}[x]$?

§2 Radical Ideals and the Ideal–Variety Correspondence

To further explore the relation between ideals and varieties, it is natural to recast Hilbert's Nullstellensatz in terms of ideals. Can we characterize the kinds of ideals that appear as the ideal of a variety? In other words, can we identify those ideals that consist of *all* polynomials which vanish on some variety V? The key observation is contained in the following simple lemma.

Lemma 1. *Let V be a variety. If $f^m \in \mathbf{I}(V)$, then $f \in \mathbf{I}(V)$.*

Proof. Let $a \in V$. If $f^m \in \mathbf{I}(V)$, then $(f(a))^m = 0$. But this can happen only if $f(a) = 0$. Since $a \in V$ was arbitrary, we must have $f \in \mathbf{I}(V)$. □

Thus, an ideal consisting of *all* polynomials which vanish on a variety V has the property that if some power of a polynomial belongs to the ideal, then the polynomial itself must belong to the ideal. This leads to the following definition.

Definition 2. An ideal I is **radical** if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.

Rephrasing Lemma 1 in terms of radical ideals gives the following statement.

Corollary 3. $\mathbf{I}(V)$ *is a radical ideal.*

On the other hand, Hilbert's Nullstellensatz tells us that the only way that an arbitrary ideal I can fail to be the ideal of all polynomials vanishing on $\mathbf{V}(I)$ is for I to contain powers f^m of polynomials f which are not in I—in other words, for I to fail to be a radical ideal. This suggests that there is a one-to-one correspondence between affine varieties and radical ideals. To clarify this and get a sharp statement, it is useful to introduce the operation of taking the radical of an ideal.

Definition 4. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. The **radical** of I, denoted $\sqrt{I}$, is the set

$$\{f \mid f^m \in I \text{ for some integer } m \geq 1\}.$$

Note that we always have $I \subseteq \sqrt{I}$ since $f \in I$ implies $f^1 \in I$ and, hence, $f \in \sqrt{I}$ by definition. It is an easy exercise to show that an ideal I is radical if and only if $I = \sqrt{I}$. A somewhat more surprising fact is that the radical of an ideal is always an ideal. To see what is at stake here, consider, for example, the ideal $J = \langle x^2, y^3 \rangle \subseteq k[x, y]$. Although neither x nor y belongs to J, it is clear that $x \in \sqrt{J}$ and $y \in \sqrt{J}$. Note that $(x \cdot y)^2 = x^2y^2 \in J$ since $x^2 \in J$; thus, $x \cdot y \in \sqrt{J}$. It is less obvious that $x + y \in \sqrt{J}$. To see this, observe that

$$(x + y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4 \in J$$

because $x^4, 4x^3y, 6x^2y^2 \in J$ (they are all multiples of x^2) and $4xy^3, y^4 \in J$ (because they are multiples of y^3). Thus, $x + y \in \sqrt{J}$. By way of contrast, neither xy nor $x + y$ belong to J.

Lemma 5. *If I is an ideal in $k[x_1, \ldots, x_n]$, then $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$ containing I. Furthermore, $\sqrt{I}$ is a radical ideal.*

Proof. We have already shown that $I \subseteq \sqrt{I}$. To show $\sqrt{I}$ is an ideal, suppose $f, g \in \sqrt{I}$. Then there are positive integers m and l such that $f^m, g^l \in I$. In the binomial expansion of $(f + g)^{m+l-1}$ every term has a factor $f^i g^j$ with $i + j = m + l - 1$. Since either $i \geq m$ or $j \geq l$, either f^i or g^j is in I, whence $f^i g^j \in I$ and every term in the binomial expansion is in I. Hence, $(f+g)^{m+l-1} \in I$ and, therefore, $f+g \in \sqrt{I}$. Finally, suppose $f \in \sqrt{I}$ and $h \in k[x_1, \ldots, x_n]$. Then $f^m \in I$ for some integer $m \geq 1$. Since I is an ideal, we have $(h \cdot f)^m = h^m f^m \in I$. Hence, $hf \in \sqrt{I}$. This shows that $\sqrt{I}$ is an ideal. In Exercise 4, you will show that $\sqrt{I}$ is a radical ideal. □

We are now ready to state the ideal-theoretic form of the Nullstellensatz.

Theorem 6 (The Strong Nullstellensatz). *Let k be an algebraically closed field. If I is an ideal in $k[x_1, \ldots, x_n]$, then*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Proof. We certainly have $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$ because $f \in \sqrt{I}$ implies that $f^m \in I$ for some m. Hence, f^m vanishes on $\mathbf{V}(I)$, which implies that f vanishes on $\mathbf{V}(I)$. Thus, $f \in \mathbf{I}(\mathbf{V}(I))$.

Conversely, take $f \in \mathbf{I}(\mathbf{V}(I))$. Then, by definition, f vanishes on $\mathbf{V}(I)$. By Hilbert's Nullstellensatz, there exists an integer $m \geq 1$ such that $f^m \in I$. But this means that $f \in \sqrt{I}$. Since f was arbitrary, $\mathbf{I}(\mathbf{V}(I)) \subseteq \sqrt{I}$, and we are done. □

It has become a custom, to which we shall adhere, to refer to Theorem 6 as *the* Nullstellensatz with no further qualification. The most important consequence of the Nullstellensatz is that it allows us to set up a "dictionary" between geometry and algebra. The basis of the dictionary is contained in the following theorem.

Theorem 7 (The Ideal–Variety Correspondence). *Let k be an arbitrary field.*

(i) *The maps*

$$\text{affine varieties} \xrightarrow{\mathbf{I}} \text{ideals}$$

and

$$\text{ideals} \xrightarrow{\mathbf{V}} \text{affine varieties}$$

are inclusion-reversing, i.e., if $I_1 \subseteq I_2$ are ideals, then $\mathbf{V}(I_1) \supseteq \mathbf{V}(I_2)$ and, similarly, if $V_1 \subseteq V_2$ are varieties, then $\mathbf{I}(V_1) \supseteq \mathbf{I}(V_2)$.

(ii) *For any variety V,*

$$\mathbf{V}(\mathbf{I}(V)) = V,$$

so that $\mathbf{I}$ is always one-to-one. On the other hand, any ideal I satisfies

$$\mathbf{V}(\sqrt{I}) = \mathbf{V}(I).$$

(iii) *If k is algebraically closed, and if we restrict to radical ideals, then the maps*

$$\text{affine varieties} \xrightarrow{\mathbf{I}} \text{radical ideals}$$

and

$$\text{radical ideals} \xrightarrow{\mathbf{V}} \text{affine varieties}$$

are inclusion-reversing bijections which are inverses of each other.

Proof. (i) The proof will be covered in the exercises.

(ii) Let $V = \mathbf{V}(f_1, \ldots, f_s)$ be an affine variety in k^n. Since every $f \in \mathbf{I}(V)$ vanishes on V, the inclusion $V \subseteq \mathbf{V}(\mathbf{I}(V))$ follows directly from the definition of $\mathbf{V}$. Going the other way, note that $f_1, \ldots, f_s \in \mathbf{I}(V)$ by the definition of $\mathbf{I}$, and, thus, $\langle f_1, \ldots, f_s \rangle \subseteq \mathbf{I}(V)$. Since $\mathbf{V}$ is inclusion-reversing, it follows that $\mathbf{V}(\mathbf{I}(V)) \subseteq \mathbf{V}(\langle f_1, \ldots, f_s \rangle) = V$. This proves that $\mathbf{V}(\mathbf{I}(V)) = V$, and, consequently, $\mathbf{I}$ is one-to-one since it has a left inverse. The final assertion of part (ii) is left as an exercise.

(iii) Since $\mathbf{I}(V)$ is radical by Corollary 3, we can think of $\mathbf{I}$ as a function which takes varieties to radical ideals. Furthermore, we already know $\mathbf{V}(\mathbf{I}(V)) = V$ for any variety V. It remains to prove $\mathbf{I}(\mathbf{V}(I)) = I$ whenever I is a radical ideal. This is easy: the Nullstellensatz tells us $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$, and I being radical implies $\sqrt{I} = I$ (see Exercise 4). This gives the desired equality. Hence, $\mathbf{V}$ and $\mathbf{I}$ are inverses of each other and, thus, define bijections between the set of radical ideals and affine varieties. The theorem is proved. $\square$

As a consequence of this theorem, any question about varieties can be rephrased as an algebraic question about radical ideals (and conversely), provided that we are working over an algebraically closed field. This ability to pass between algebra and geometry will give us considerable power.

In view of the Nullstellensatz and the importance it assigns to radical ideals, it is natural to ask whether one can compute generators for the radical from generators of the original ideal. In fact, there are three questions to ask concerning an ideal $I = \langle f_1, \ldots, f_s \rangle$:

- (Radical Generators) Is there an algorithm which produces a set $\{g_1, \ldots, g_m\}$ of polynomials such that $\sqrt{I} = \langle g_1, \ldots, g_m \rangle$?
- (Radical Ideal) Is there an algorithm which will determine whether I is radical?
- (Radical Membership) Given $f \in k[x_1, \ldots, x_n]$, is there an algorithm which will determine whether $f \in \sqrt{I}$?

The existence of these algorithms follows from the work of HERMANN (1926) [see also MINES, RICHMAN, and RUITENBERG (1988) and SEIDENBERG (1974, 1984) for more modern expositions]. More practical algorithms for finding radicals follow from the work of GIANNI, TRAGER and ZACHARIAS (1988), KRICK and LOGAR (1991), and EISENBUD, HUNEKE and VASCONCELOS (1992). These algorithms have been implemented in CoCoA, Singular, and Macaulay2, among others. See, for example, Section 4.5 of GREUEL and PFISTER (2008).

For now, we will settle for solving the more modest *radical membership problem*. To test whether $f \in \sqrt{I}$, we could use the ideal membership algorithm to check whether $f^m \in I$ for all integers $m > 0$. This is not satisfactory because we might have to go to very large powers of m, and it will never tell us if $f \notin \sqrt{I}$ (at least, not until we work out *a priori* bounds on m). Fortunately, we can adapt the proof of Hilbert's Nullstellensatz to give an algorithm for determining whether $f \in \sqrt{\langle f_1, \ldots, f_s \rangle}$.

Proposition 8 (Radical Membership). *Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant* *polynomial* 1 *belongs to the ideal* $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq k[x_1, \ldots, x_n, y]$, *in which case* $\tilde{I} = k[x_1, \ldots, x_n, y]$.

Proof. From equations (2), (3), and (4) in the proof of Hilbert's Nullstellensatz in §1, we see that $1 \in \tilde{I}$ implies $f^m \in I$ for some m, which, in turn, implies $f \in \sqrt{I}$. Going the other way, suppose that $f \in \sqrt{I}$. Then $f^m \in I \subseteq \tilde{I}$ for some m. But we also have $1 - yf \in \tilde{I}$, and, consequently,

$$1 = y^m f^m + (1 - y^m f^m) = y^m \cdot f^m + (1 - yf) \cdot (1 + yf + \cdots + y^{m-1} f^{m-1}) \in \tilde{I},$$

as desired. $\square$

Proposition 8, together with our earlier remarks on determining whether 1 belongs to an ideal (see the discussion of the consistency problem in §1), immediately leads to the following **radical membership algorithm**: to determine if $f \in \sqrt{\langle f_1, \ldots, f_s \rangle} \subseteq k[x_1, \ldots, x_n]$, we compute a reduced Gröbner basis of the ideal $\langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq k[x_1, \ldots, x_n, y]$ with respect to some ordering. If the result is $\{1\}$, then $f \in \sqrt{I}$. Otherwise, $f \notin \sqrt{I}$.

As an example, consider the ideal $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle$ in $k[x, y]$. Let us test if $f = y - x^2 + 1$ lies in $\sqrt{I}$. Using lex order on $k[x, y, z]$, one checks that the ideal

$$\tilde{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) \rangle \subseteq k[x, y, z]$$

has reduced Gröbner basis $\{1\}$. It follows that $y - x^2 + 1 \in \sqrt{I}$ by Proposition 8. Using the division algorithm, we can check what power of $y - x^2 + 1$ lies in I:

$$\begin{aligned} \overline{y - x^2 + 1}^G &= y - x^2 + 1, \\ \overline{(y - x^2 + 1)^2}^G &= -2x^2 y + 2y, \\ \overline{(y - x^2 + 1)^3}^G &= 0, \end{aligned}$$

where $G = \{x^4 - 2x^2 + 1, y^2\}$ is a Gröbner basis of I with respect to lex order and $\overline{p}^G$ is the remainder of p on division by G. As a consequence, we see that $(y - x^2 + 1)^3 \in I$, but no lower power of $y - x^2 + 1$ is in I (in particular, $y - x^2 + 1 \notin I$).

We can also see what is happening in this example geometrically. As a set, $\mathbf{V}(I) = \{(\pm 1, 0)\}$, but (speaking somewhat imprecisely) every polynomial in I vanishes to order at least 2 at each of the two points in $\mathbf{V}(I)$. This is visible from the form of the generators of I if we factor them:

$$xy^2 + 2y^2 = y^2(x + 2) \quad \text{and} \quad x^4 - 2x^2 + 1 = (x^2 - 1)^2.$$

Even though $f = y - x^2 + 1$ also vanishes at $(\pm 1, 0)$, f only vanishes to order 1 there. We must take a higher power of f to obtain an element of I.

We will end this section with a discussion of the one case where we can compute the radical of an ideal, which is when we are dealing with a principal ideal $I = \langle f \rangle$. A nonconstant polynomial f is said to be *irreducible* if it has the property that whenever $f = g \cdot h$ for some polynomials g and h, then either g or h is a constant. As noted in §2 of Appendix A, any nonconstant polynomial f can always be written as a product of irreducible polynomials. By collecting the irreducible polynomials which differ by constant multiples of one another, we can write f in the form

$$f = cf_1^{a_1} \cdots f_r^{a_r}, \quad c \in k,$$

where the f_i's, $1 \leq i \leq r$, are *distinct* irreducible polynomials, meaning that f_i and f_j are not constant multiples of one another whenever $i \neq j$. Moreover, this expression for f is *unique* up to reordering the f_i's and up to multiplying the f_i's by constant multiples. (This *unique factorization* is Theorem 2 from Appendix A, §2.)

If we have f expressed as a product of irreducible polynomials, then it is easy to write down the radical of the principal ideal generated by f.

Proposition 9. *Let $f \in k[x_1, \ldots, x_n]$ and $I = \langle f \rangle$ be the principal ideal generated by f. If $f = cf_1^{a_1} \cdots f_r^{a_r}$ is the factorization of f into a product of distinct irreducible polynomials, then*

$$\sqrt{I} = \sqrt{\langle f \rangle} = \langle f_1 f_2 \cdots f_r \rangle.$$

Proof. We first show that $f_1 f_2 \cdots f_r$ belongs to $\sqrt{I}$. Let N be an integer strictly greater than the maximum of $a_1, \ldots, a_r$. Then

$$(f_1 f_2 \cdots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \cdots f_r^{N-a_r} f$$

is a polynomial multiple of f. This shows that $(f_1 f_2 \cdots f_r)^N \in I$, which implies that $f_1 f_2 \cdots f_r \in \sqrt{I}$. Thus $\langle f_1 f_2 \cdots f_r \rangle \subseteq \sqrt{I}$.

Conversely, suppose that $g \in \sqrt{I}$. Then there exists a positive integer M such that $g^M \in I = \langle f \rangle$, so that g^M is a multiple of f and hence a multiple of each irreducible factor f_i of f. Thus, f_i is an irreducible factor of g^M. However, the unique factorization of g^M into distinct irreducible polynomials is the Mth power of the factorization of g. It follows that each f_i is an irreducible factor of g. This implies that g is a polynomial multiple of $f_1 f_2 \cdots f_r$ and, therefore, g is contained in the ideal $\langle f_1 f_2 \cdots f_r \rangle$. The proposition is proved. □

In view of Proposition 9, we make the following definition:

Definition 10. If $f \in k[x_1, \ldots, x_n]$ is a polynomial, we define the **reduction** of f, denoted f_{red}, to be the polynomial such that $\langle f_{\mathrm{red}} \rangle = \sqrt{\langle f \rangle}$. A polynomial is said to be **reduced** (or **square-free**) if $f = f_{\mathrm{red}}$.

Thus, f_{red} is the polynomial f with repeated factors "stripped away." So, for example, if $f = (x + y^2)^3(x - y)$, then $f_{\mathrm{red}} = (x + y^2)(x - y)$. Note that f_{red} is only unique up to a constant factor in k.

The usefulness of Proposition 9 is mitigated by the requirement that f be factored into irreducible factors. We might ask if there is an algorithm to compute f_{red} from f without factoring f first. It turns out that such an algorithm exists.

To state the algorithm, we will need the notion of a greatest common divisor of two polynomials.

Definition 11. Let $f, g \in k[x_1, \ldots, x_n]$. Then $h \in k[x_1, \ldots, x_n]$ is called a **greatest common divisor** of f and g, and denoted $h = \gcd(f, g)$, if

(i) h divides f and g.
(ii) If p is any polynomial that divides both f and g, then p divides h.

It is easy to show that $\gcd(f,g)$ exists and is unique up to multiplication by a nonzero constant in k (see Exercise 9). Unfortunately, the one-variable algorithm for finding the gcd (i.e., the Euclidean Algorithm) does not work in the case of several variables. To see this, consider the polynomials xy and xz in $k[x,y,z]$. Clearly, $\gcd(xy,xz) = x$. However, no matter what term ordering we use, dividing xy by xz gives 0 plus remainder xy and dividing xz by xy gives 0 plus remainder xz. As a result, neither polynomial "reduces" with respect to the other and there is no next step to which to apply the analogue of the Euclidean Algorithm.

Nevertheless, there is an algorithm for calculating the gcd of two polynomials in several variables. We defer a discussion of it until the next section after we have studied intersections of ideals. For the purposes of our discussion here, let us assume that we have such an algorithm. We also remark that given polynomials $f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$, one can define $\gcd(f_1,f_2,\ldots,f_s)$ exactly as in the one-variable case. There is also an algorithm for computing $\gcd(f_1,f_2,\ldots,f_s)$.

Using this notion of gcd, we can now give a formula for computing the radical of a principal ideal.

Proposition 12. *Suppose that k is a field containing the rational numbers $\mathbb{Q}$ and let $I = \langle f\rangle$ be a principal ideal in $k[x_1,\ldots,x_n]$. Then $\sqrt{I} = \langle f_{\mathrm{red}}\rangle$, where*

$$f_{\mathrm{red}} = \frac{f}{\gcd\left(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}\right)}.$$

Proof. Writing f as in Proposition 9, we know that $\sqrt{I} = \langle f_1 f_2\cdots f_r\rangle$. Thus, it suffices to show that

$$\gcd\Big(f, \frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\Big) = f_1^{a_1-1} f_2^{a_2-1}\cdots f_r^{a_r-1}. \tag{1}$$

We first use the product rule to note that

$$\frac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1}\cdots f_r^{a_r-1}\Big(a_1\frac{\partial f_1}{\partial x_j} f_2\cdots f_r + \cdots + a_r f_1\cdots f_{r-1}\frac{\partial f_r}{\partial x_j}\Big).$$

This proves that $f_1^{a_1-1} f_2^{a_2-1}\cdots f_r^{a_r-1}$ divides the gcd. It remains to show that for each i, there is some $\frac{\partial f}{\partial x_j}$ which is not divisible by $f_i^{a_i}$.

Write $f = f_i^{a_i} h_i$, where h_i is not divisible by f_i. Since f_i is nonconstant, some variable x_j must appear in f_i. The product rule gives us

$$\frac{\partial f}{\partial x_j} = f_i^{a_i-1}\Big(a_1\frac{\partial f_i}{\partial x_j} h_i + f_i\frac{\partial h_i}{\partial x_j}\Big).$$

If this expression is divisible by $f_i^{a_i}$, then $\frac{\partial f_i}{\partial x_j} h_i$ must be divisible by f_i. Since f_i is irreducible and does not divide h_i, this forces f_i to divide $\frac{\partial f_i}{\partial x_j}$. In Exercise 13, you will show that $\frac{\partial f_i}{\partial x_j}$ is nonzero since $\mathbb{Q} \subseteq k$ and x_j appears in f_i. As $\frac{\partial f_i}{\partial x_j}$ also has smaller total degree than f_i, it follows that f_i cannot divide $\frac{\partial f_i}{\partial x_j}$. Consequently, $\frac{\partial f}{\partial x_j}$ is not divisible by $f_i^{a_i}$, which proves (1), and the proposition follows. $\square$

It is worth remarking that for fields which do not contain $\mathbb{Q}$, the above formula for f_{red} may fail (see Exercise 13).

EXERCISES FOR §2

1. Given a field k (not necessarily algebraically closed), show that $\sqrt{\langle x^2, y^2 \rangle} = \langle x, y \rangle$ and, more generally, show that $\sqrt{\langle x^n, y^m \rangle} = \langle x, y \rangle$ for any positive integers n and m.
2. Let f and g be distinct nonconstant polynomials in $k[x, y]$ and let $I = \langle f^2, g^3 \rangle$. Is it necessarily true that $\sqrt{I} = \langle f, g \rangle$? Explain.
3. Show that $\langle x^2 + 1 \rangle \subseteq \mathbb{R}[x]$ is a radical ideal, but that $\mathbf{V}(x^2 + 1)$ is the empty variety.
4. Let I be an ideal in $k[x_1, \dots, x_n]$, where k is an arbitrary field.
   a. Show that $\sqrt{I}$ is a radical ideal.
   b. Show that I is radical if and only if $I = \sqrt{I}$.
   c. Show that $\sqrt{\sqrt{I}} = \sqrt{I}$.
5. Prove that $\mathbf{I}$ and $\mathbf{V}$ are inclusion-reversing and that $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$ for any ideal I.
6. Let I be an ideal in $k[x_1, \dots, x_n]$.
   a. In the special case when $\sqrt{I} = \langle f_1, f_2 \rangle$, with $f_i^{m_i} \in I$, prove that $f^{m_1+m_2-1} \in I$ for all $f \in \sqrt{I}$.
   b. Now prove that for any I, there exists a single integer m such that $f^m \in I$ for all $f \in \sqrt{I}$. Hint: Write $\sqrt{I} = \langle f_1, \dots, f_s \rangle$.
7. Determine whether the following polynomials lie in the following radicals. If the answer is yes, what is the smallest power of the polynomial that lies in the ideal?
   a. Is $x + y \in \sqrt{\langle x^3, y^3, xy(x + y) \rangle}$?
   b. Is $x^2 + 3xz \in \sqrt{\langle x + z, x^2y, x - z^2 \rangle}$?
8. Let $f_1 = y^2 + 2xy - 1$ and $f_2 = x^2 + 1$. Prove that $\langle f_1, f_2 \rangle$ is not a radical ideal. Hint: What is $f_1 + f_2$?
9. Given $f, g \in k[x_1, \dots, x_n]$, use unique factorization to prove that $\gcd(f, g)$ exists. Also prove that $\gcd(f, g)$ is unique up to multiplication by a nonzero constant of k.
10. Prove the following ideal-theoretic characterization of $\gcd(f, g)$: given polynomials f, g, h in $k[x_1, \dots, x_n]$, then $h = \gcd(f, g)$ if and only if h is a generator of the smallest principal ideal containing $\langle f, g \rangle$ (i.e., if $\langle h \rangle \subseteq J$, whenever J is a principal ideal such that $J \supseteq \langle f, g \rangle$).
11. Find a basis for the ideal
$$\sqrt{\langle x^5 - 2x^4 + 2x^2 - x, x^5 - x^4 - 2x^3 + 2x^2 + x - 1 \rangle}.$$
Compare with Exercise 17 of Chapter 1, §5.
12. Let $f = x^5+3x^4y+3x^3y^2-2x^4y^2+x^2y^3-6x^3y^3-6x^2y^4+x^3y^4-2xy^5+3x^2y^5+3xy^6+y^7 \in \mathbb{Q}[x, y]$. Compute $\sqrt{\langle f \rangle}$.
13. A field k has *characteristic zero* if it contains the rational numbers $\mathbb{Q}$; otherwise, k has *positive characteristic*.
   a. Let k be the field $\mathbb{F}_2$ from Exercise 1 of Chapter 1, §1. If $f = x_1^2 + \cdots + x_n^2 \in \mathbb{F}_2[x_1, \dots, x_n]$, then show that $\frac{\partial f}{\partial x_i} = 0$ for all i. Conclude that the formula given in Proposition 12 may fail when the field is $\mathbb{F}_2$.

b. Let k be a field of characteristic zero and let $f \in k[x_1, \ldots, x_n]$ be nonconstant. If the variable x_j appears in f, then prove that $\frac{\partial f}{\partial x_j} \neq 0$. Also explain why $\frac{\partial f}{\partial x_j}$ has smaller total degree than f.

14. Let $J = \langle xy, (x-y)x \rangle$. Describe $\mathbf{V}(J)$ and show that $\sqrt{J} = \langle x \rangle$.
15. Prove that $I = \langle xy, xz, yz \rangle$ is a radical ideal. Hint: If you divide $f \in k[x,y,z]$ by xy, xz, yz, what does the remainder look like? What does f^m look like?
16. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Assume that I has a Gröbner basis $G = \{g_1, \ldots, g_t\}$ such that for all i, $\text{LT}(g_i)$ is square-free in the sense of Definition 10.
    a. If $f \in \sqrt{I}$, prove that $\text{LT}(f)$ is divisible by $\text{LT}(g_i)$ for some i. Hint: $f^m \in I$.
    b. Prove that I is radical. Hint: Use part (a) to show that G is a Gröbner basis of $\sqrt{I}$.
17. This exercise continues the line of thought begun in Exercise 16.
    a. Prove that a monomial ideal in $k[x_1, \ldots, x_n]$ is radical if and only if its minimal generators are square-free.
    b. Given an ideal $I \subseteq k[x_1, \ldots, x_n]$, prove that if $\langle \text{LT}(I) \rangle$ is radical, then I is radical.
    c. Give an example to show that the converse of part (b) can fail.

§3 Sums, Products, and Intersections of Ideals

Ideals are algebraic objects and, as a result, there are natural algebraic operations we can define on them. In this section, we consider three such operations: sum, intersection, and product. These are binary operations: to each pair of ideals, they associate a new ideal. We shall be particularly interested in two general questions which arise in connection with each of these operations. The first asks how, given generators of a pair of ideals, one can compute generators of the new ideals which result on applying these operations. The second asks for the geometric significance of these algebraic operations. Thus, the first question fits the general computational theme of this book; the second, the general thrust of this chapter. We consider each of the operations in turn.

Sums of Ideals

Definition 1. If I and J are ideals of the ring $k[x_1, \ldots, x_n]$, then the **sum** of I and J, denoted $I + J$, is the set

$$I + J = \{f + g \mid f \in I \text{ and } g \in J\}.$$

Proposition 2. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $I + J$ is also an ideal in $k[x_1, \ldots, x_n]$. In fact, $I + J$ is the smallest ideal containing I and J. Furthermore, if $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.*

Proof. Note first that $0 = 0 + 0 \in I + J$. Suppose $h_1, h_2 \in I + J$. By the definition of $I + J$, there exist $f_1, f_2 \in I$ and $g_1, g_2 \in J$ such that $h_1 = f_1 + g_1, h_2 = f_2 + g_2$. Then, after rearranging terms slightly, $h_1 + h_2 = (f_1 + f_2) + (g_1 + g_2)$. But $f_1 + f_2 \in I$ because I is an ideal and, similarly, $g_1 + g_2 \in J$, whence $h_1 + h_2 \in I + J$. To check closure under multiplication, let $h \in I + J$ and $p \in k[x_1, \ldots, x_n]$ be any polynomial. Then, as above, there exist $f \in I$ and $g \in J$ such that $h = f + g$. But then $p \cdot h = p \cdot (f + g) = p \cdot f + p \cdot g$. Now $p \cdot f \in I$ and $p \cdot g \in J$ because I and J are ideals. Consequently, $p \cdot h \in I + J$. This shows that $I + J$ is an ideal.

If H is an ideal which contains I and J, then H must contain all elements $f \in I$ and $g \in J$. Since H is an ideal, H must contain all $f + g$, where $f \in I, g \in J$. In particular, $H \supseteq I + J$. Therefore, every ideal containing I and J contains $I + J$ and, thus, $I + J$ must be the smallest such ideal.

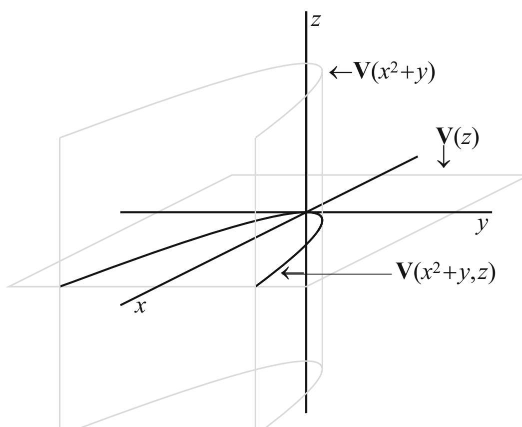
Finally, if $I = \langle f_1, \ldots, f_r \rangle$ and $J = \langle g_1, \ldots, g_s \rangle$, then $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$ is an ideal containing I and J, so that $I + J \subseteq \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. The reverse inclusion is obvious, so that $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. □

The following corollary is an immediate consequence of Proposition 2.

Corollary 3. *If $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$, then*

$$\langle f_1, \ldots, f_r \rangle = \langle f_1 \rangle + \cdots + \langle f_r \rangle.$$

To see what happens geometrically, let $I = \langle x^2 + y \rangle$ and $J = \langle z \rangle$ be ideals in $\mathbb{R}[x, y, z]$. We have sketched $\mathbf{V}(I)$ and $\mathbf{V}(J)$ on the next page. Then $I + J = \langle x^2 + y, z \rangle$ contains both $x^2 + y$ and z. Thus, the variety $\mathbf{V}(I + J)$ must consist of those points where both $x^2 + y$ and z vanish, i.e., it must be the intersection of $\mathbf{V}(I)$ and $\mathbf{V}(J)$.



The same line of reasoning generalizes to show that addition of ideals corresponds geometrically to taking intersections of varieties.

Theorem 4. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$.*

Proof. If $a \in \mathbf{V}(I + J)$, then $a \in \mathbf{V}(I)$ because $I \subseteq I + J$; similarly, $a \in \mathbf{V}(J)$. Thus, $a \in \mathbf{V}(I) \cap \mathbf{V}(J)$ and we conclude that $\mathbf{V}(I + J) \subseteq \mathbf{V}(I) \cap \mathbf{V}(J)$.

To get the opposite inclusion, suppose $a \in \mathbf{V}(I) \cap \mathbf{V}(J)$. Let h be any polynomial in $I + J$. Then there exist $f \in I$ and $g \in J$ such that $h = f + g$. We have $f(a) = 0$ because $a \in \mathbf{V}(I)$ and $g(a) = 0$ because $a \in \mathbf{V}(J)$. Thus, $h(a) = f(a) + g(a) = 0 + 0 = 0$. Since h was arbitrary, we conclude that $a \in \mathbf{V}(I + J)$. Hence, $\mathbf{V}(I + J) \supseteq \mathbf{V}(I) \cap \mathbf{V}(J)$. □

An analogue of Theorem 4 stated in terms of generators was given in Lemma 2 of Chapter 1, §2.

Products of Ideals

In Lemma 2 of Chapter 1, §2, we encountered the fact that an ideal generated by the products of the generators of two other ideals corresponds to the union of varieties:

$$\mathbf{V}(f_1,\ldots,f_r)\cup\mathbf{V}(g_1,\ldots,g_s)=\mathbf{V}(f_ig_j, 1\le i\le r, 1\le j\le s).$$

Thus, for example, the variety $\mathbf{V}(xz, yz)$ corresponding to an ideal generated by the product of the generators of the ideals, $\langle x, y\rangle$ and $\langle z\rangle$ in $k[x, y, z]$ is the union of $\mathbf{V}(x, y)$ (the z-axis) and $\mathbf{V}(z)$ [the (x, y)-plane]. This suggests the following definition.

Definition 5. If I and J are two ideals in $k[x_1,\ldots,x_n]$, then their **product**, denoted $I\cdot J$, is defined to be the ideal generated by all polynomials $f\cdot g$ where $f\in I$ and $g\in J$.

Thus, the product $I\cdot J$ of I and J is the set

$$I\cdot J=\{f_1g_1+\cdots+f_rg_r \mid f_1,\ldots,f_r\in I,\ g_1,\ldots,g_r\in J,\ r \text{ a positive integer}\}.$$

To see that this is an ideal, note that $0=0\cdot 0\in I\cdot J$. Moreover, it is clear that $h_1, h_2\in I\cdot J$ implies that $h_1+h_2\in I\cdot J$. Finally, if $h=f_1g_1+\cdots+f_rg_r\in I\cdot J$ and p is any polynomial, then

$$ph=(pf_1)g_1+\cdots+(pf_r)g_r\in I\cdot J$$

since $pf_i\in I$ for all i, $1\le i\le r$. Note that the set of products would not be an ideal because it would not be closed under addition. The following easy proposition shows that computing a set of generators for $I\cdot J$ given sets of generators for I and J is completely straightforward.

Proposition 6. *Let $I=\langle f_1,\ldots,f_r\rangle$ and $J=\langle g_1,\ldots,g_s\rangle$. Then $I\cdot J$ is generated by the set of all products of generators of I and J:*

$$I\cdot J=\langle f_ig_j \mid 1\le i\le r, 1\le j\le s\rangle.$$

Proof. It is clear that the ideal generated by products f_ig_j of the generators is contained in $I\cdot J$. To establish the opposite inclusion, note that any polynomial in $I\cdot J$ is a sum of polynomials of the form fg with $f\in I$ and $g\in J$. But we can write f and g in terms of the generators $f_1,\ldots,f_r$ and $g_1,\ldots,g_s$, respectively, as

$$f=a_1f_1+\cdots+a_rf_r,\quad g=b_1g_1+\cdots+b_sg_s$$

for appropriate polynomials $a_1,\ldots,a_r, b_1,\ldots,b_s$. Thus, fg, and consequently any sum of polynomials of this form, can be written as a sum $\sum_{ij}c_{ij}f_ig_j$, where $c_{ij}\in k[x_1,\ldots,x_n]$. □

The following proposition guarantees that the product of ideals does indeed correspond geometrically to the operation of taking the union of varieties.

Theorem 7. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbf{V}(I \cdot J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

Proof. Let $a \in \mathbf{V}(I \cdot J)$. Then $g(a)h(a) = 0$ for all $g \in I$ and all $h \in J$. If $g(a) = 0$ for all $g \in I$, then $a \in \mathbf{V}(I)$. If $g(a) \neq 0$ for some $g \in I$, then we must have $h(a) = 0$ for all $h \in J$. In either event, $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$.

Conversely, suppose $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Either $g(a) = 0$ for all $g \in I$ or $h(a) = 0$ for all $h \in J$. Thus, $g(a)h(a) = 0$ for all $g \in I$ and $h \in J$. Thus, $f(a) = 0$ for all $f \in I \cdot J$ and, hence, $a \in \mathbf{V}(I \cdot J)$. □

In what follows, we will often write the product of ideals as IJ rather than $I \cdot J$.

Intersections of Ideals

The operation of forming the intersection of two ideals is, in some ways, even more primitive than the operations of addition and multiplication.

Definition 8. The **intersection** $I \cap J$ of two ideals I and J in $k[x_1, \ldots, x_n]$ is the set of polynomials which belong to both I and J.

As in the case of sums, the set of ideals is closed under intersections.

Proposition 9. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $I \cap J$ is also an ideal.*

Proof. Note that $0 \in I \cap J$ since $0 \in I$ and $0 \in J$. If $f, g \in I \cap J$, then $f + g \in I$ because $f, g \in I$. Similarly, $f + g \in J$ and, hence, $f + g \in I \cap J$. Finally, to check closure under multiplication, let $f \in I \cap J$ and h be any polynomial in $k[x_1, \ldots, x_n]$. Since $f \in I$ and I is an ideal, we have $h \cdot f \in I$. Similarly, $h \cdot f \in J$ and, hence, $h \cdot f \in I \cap J$. □

Note that we always have $IJ \subseteq I \cap J$ since elements of IJ are sums of polynomials of the form fg with $f \in I$ and $g \in J$. But the latter belongs to both I (since $f \in I$) and J (since $g \in J$). However, IJ can be strictly contained in $I \cap J$. For example, if $I = J = \langle x, y \rangle$, then $IJ = \langle x^2, xy, y^2 \rangle$ is strictly contained in $I \cap J = I = \langle x, y \rangle$ ($x \in I \cap J$, but $x \notin IJ$).

Given two ideals and a set of generators for each, we would like to be able to compute a set of generators for the intersection. This is much more delicate than the analogous problems for sums and products of ideals, which were entirely straightforward. To see what is involved, suppose I is the ideal in $\mathbb{Q}[x, y]$ generated by the polynomial $f = (x + y)^4(x^2 + y)^2(x - 5y)$ and let J be the ideal generated by the polynomial $g = (x + y)(x^2 + y)^3(x + 3y)$. We leave it as an (easy) exercise to check that

$$I \cap J = \langle (x + y)^4(x^2 + y)^3(x - 5y)(x + 3y) \rangle.$$

This computation is easy precisely because we were given factorizations of f and g into irreducible polynomials. In general, such factorizations may not be available. So any algorithm which allows one to compute intersections will have to be powerful enough to circumvent this difficulty.

Nevertheless, there is a nice trick that reduces the computation of intersections to computing the intersection of an ideal with a subring (i.e., eliminating variables), a problem which we have already solved. To state the theorem, we need a little notation: if I is an ideal in $k[x_1, \ldots, x_n]$ and $f(t) \in k[t]$ a polynomial in the single variable t, then $f(t)I$ denotes the ideal in $k[x_1, \ldots, x_n, t]$ generated by the set of polynomials $\{f(t) \cdot h \mid h \in I\}$. This is a little different from our usual notion of product in that the ideal I and the ideal generated by $f(t)$ in $k[t]$ lie in different rings: in fact, the ideal $I \subseteq k[x_1, \ldots, x_n]$ is *not* an ideal in $k[x_1, \ldots, x_n, t]$ because it is not closed under multiplication by t. When we want to stress that a polynomial $h \in k[x_1, \ldots, x_n]$ involves only the variables $x_1, \ldots, x_n$, we write $h = h(x)$. Along the same lines, if we are considering a polynomial g in $k[x_1, \ldots, x_n, t]$ and we want to emphasize that it can involve the variables $x_1, \ldots, x_n$ as well as t, we will write $g = g(x, t)$. In terms of this notation, $f(t)I = \langle f(t)h(x) \mid h(x) \in I\rangle$. So, for example, if $f(t) = t^2 - t$ and $I = \langle x, y\rangle$, then the ideal $f(t)I$ in $k[x, y, t]$ contains $(t^2 - t)x$ and $(t^2 - t)y$. In fact, it is not difficult to see that $f(t)I$ is generated as an ideal by $(t^2 - t)x$ and $(t^2 - t)y$. This is a special case of the following assertion.

Lemma 10.

(i) *If I is generated as an ideal in $k[x_1, \ldots, x_n]$ by $p_1(x), \ldots, p_r(x)$, then $f(t)I$ is generated as an ideal in $k[x_1, \ldots, x_n, t]$ by $f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)$.*

(ii) *If $g(x, t) \in f(t)I$ and a is any element of the field k, then $g(x, a) \in I$.*

Proof. To prove the first assertion, note that any polynomial $g(x, t) \in f(t)I$ can be expressed as a sum of terms of the form $h(x, t) \cdot f(t) \cdot p(x)$ for $h \in k[x_1, \ldots, x_n, t]$ and $p \in I$. But because I is generated by $p_1, \ldots, p_r$ the polynomial $p(x)$ can be expressed as a sum of terms of the form $q_i(x)p_i(x)$, $1 \leq i \leq r$. In other words,

$$p(x) = \sum_{i=1}^{r} q_i(x)p_i(x).$$

Hence,

$$h(x, t) \cdot f(t) \cdot p(x) = \sum_{i=1}^{r} h(x, t)q_i(x)f(t)p_i(x).$$

Now, for each i, $1 \leq i \leq r$, $h(x, t) \cdot q_i(x) \in k[x_1, \ldots, x_n, t]$. Thus, $h(x, t) \cdot f(t) \cdot p(x)$ belongs to the ideal in $k[x_1, \ldots, x_n, t]$ generated by $f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)$. Since $g(x, t)$ is a sum of such terms,

$$g(x, t) \in \langle f(t) \cdot p_1(x), \ldots, f(t) \cdot p_r(x)\rangle,$$

which establishes (i). The second assertion follows immediately upon substituting $a \in k$ for t. $\square$

Theorem 11. *Let I, J be ideals in $k[x_1, \dots, x_n]$. Then*

$$I \cap J = (tI + (1 - t)J) \cap k[x_1, \dots, x_n].$$

Proof. Note that $tI + (1 - t)J$ is an ideal in $k[x_1, \dots, x_n, t]$. To establish the desired equality, we use the usual strategy of proving containment in both directions.

Suppose $f \in I \cap J$. Since $f \in I$, we have $t \cdot f \in tI$. Similarly, $f \in J$ implies $(1 - t) \cdot f \in (1 - t)J$. Thus, $f = t \cdot f + (1 - t) \cdot f \in tI + (1 - t)J$. Since $I, J \subseteq k[x_1, \dots, x_n]$, we have $f \in (tI + (1 - t)J) \cap k[x_1, \dots, x_n]$. This shows that $I \cap J \subseteq (tI + (1 - t)J) \cap k[x_1, \dots, x_n]$.

To establish the opposite containment, take $f \in (tI + (1 - t)J) \cap k[x_1, \dots, x_n]$. Then $f(x) = g(x, t) + h(x, t)$, where $g(x, t) \in tI$ and $h(x, t) \in (1 - t)J$. First set $t = 0$. Since every element of tI is a multiple of t, we have $g(x, 0) = 0$. Thus, $f(x) = h(x, 0)$ and hence, $f(x) \in J$ by Lemma 10. On the other hand, set $t = 1$ in the relation $f(x) = g(x, t) + h(x, t)$. Since every element of $(1 - t)J$ is a multiple of $1 - t$, we have $h(x, 1) = 0$. Thus, $f(x) = g(x, 1)$ and, hence, $f(x) \in I$ by Lemma 10. Since f belongs to both I and J, we have $f \in I \cap J$. Thus, $I \cap J \supseteq (tI + (1 - t)J) \cap k[x_1, \dots, x_n]$ and this completes the proof. □

The above result and the Elimination Theorem (Theorem 2 of Chapter 3, §1) lead to the following **algorithm for computing intersections of ideals**: if $I = \langle f_1, \dots, f_r \rangle$ and $J = \langle g_1, \dots, g_s \rangle$ are ideals in $k[x_1, \dots, x_n]$, we consider the ideal

$$\langle tf_1, \dots, tf_r, (1 - t)g_1, \dots, (1 - t)g_s \rangle \subseteq k[x_1, \dots, x_n, t]$$

and compute a Gröbner basis with respect to lex order in which t is greater than the x_i. The elements of this basis which do not contain the variable t will form a basis (in fact, a Gröbner basis) of $I \cap J$. For more efficient calculations, one could also use one of the orders described in Exercises 5 and 6 of Chapter 3, §1. An algorithm for intersecting three or more ideals is described in Proposition 6.19 of BECKER and WEISPFENNING (1993).

As a simple example of the above procedure, suppose we want to compute the intersection of the ideals $I = \langle x^2y \rangle$ and $J = \langle xy^2 \rangle$ in $\mathbb{Q}[x, y]$. We consider the ideal

$$tI + (1 - t)J = \langle tx^2y, (1 - t)xy^2 \rangle = \langle tx^2y, txy^2 - xy^2 \rangle$$

in $\mathbb{Q}[t, x, y]$. Computing the S-polynomial of the generators, we obtain $tx^2y^2 - (tx^2y^2 - x^2y^2) = x^2y^2$. It is easily checked that $\{tx^2y, txy^2 - xy^2, x^2y^2\}$ is a Gröbner basis of $tI + (1 - t)J$ with respect to lex order with $t > x > y$. By the Elimination Theorem, $\{x^2y^2\}$ is a (Gröbner) basis of $(tI + (1 - t)J) \cap \mathbb{Q}[x, y]$. Thus,

$$I \cap J = \langle x^2y^2 \rangle.$$

As another example, we invite the reader to apply the algorithm for computing intersections of ideals to give an alternate proof that the intersection $I \cap J$ of the ideals

$$I = \langle (x + y)^4(x^2 + y)^2(x - 5y) \rangle \quad \text{and} \quad J = \langle (x + y)(x^2 + y)^3(x + 3y) \rangle$$

in $\mathbb{Q}[x,y]$ is

$$I \cap J = \langle (x+y)^4(x^2+y)^3(x-5y)(x+3y)\rangle.$$

These examples above are rather simple in that our algorithm applies to ideals which are not necessarily principal, whereas the examples given here involve intersections of principal ideals. We shall see a somewhat more complicated example in the exercises.

We can generalize both of the examples above by introducing the following definition.

Definition 12. A polynomial $h \in k[x_1, \ldots, x_n]$ is called a **least common multiple** of $f, g \in k[x_1, \ldots, x_n]$ and denoted $h = \mathrm{lcm}(f,g)$ if

(i) f divides h and g divides h.
(ii) If f and g both divide a polynomial p, then h divides p.

For example,

$$\mathrm{lcm}(x^2y, xy^2) = x^2y^2$$

and

$$\begin{aligned}\mathrm{lcm}((x+y)^4(x^2+y)^2(x-5y), (x+y)(x^2+y)^3(x+3y))&\\ = (x+y)^4(x^2+y)^3(x-5y)(x+3y).&\end{aligned}$$

More generally, suppose $f, g \in k[x_1, \ldots, x_n]$ and let $f = cf_1^{a_1} \ldots f_r^{a_r}$ and $g = c' g_1^{b_1} \ldots g_s^{b_s}$ be their factorizations into distinct irreducible polynomials. It may happen that some of the irreducible factors of f are constant multiples of those of g. In this case, let us suppose that we have rearranged the order of the irreducible polynomials in the expressions for f and g so that for some l, $1 \le l \le \min(r,s)$, f_i is a constant (nonzero) multiple of g_i for $1 \le i \le l$ and for all $i, j > l$, f_i is not a constant multiple of g_j. Then it follows from unique factorization that

$$\text{(1)} \qquad \mathrm{lcm}(f,g) = f_1^{\max(a_1,b_1)} \cdots f_l^{\max(a_l,b_l)} \cdot g_{l+1}^{b_{l+1}} \cdots g_s^{b_s} \cdot f_{l+1}^{a_{l+1}} \cdots f_r^{a_r}.$$

[In the case that f and g share no common factors, we have $\mathrm{lcm}(f,g) = f \cdot g$.] This, in turn, implies the following result.

Proposition 13.

(i) *The intersection $I \cap J$ of two principal ideals $I, J \subseteq k[x_1, \ldots, x_n]$ is a principal ideal.*
(ii) *If $I = \langle f \rangle$, $J = \langle g \rangle$ and $I \cap J = \langle h \rangle$, then*

$$h = \mathrm{lcm}(f,g).$$

Proof. The proof will be left as an exercise. □

This result, together with our algorithm for computing the intersection of two ideals immediately gives an **algorithm for computing the least common multiple** of two polynomials: to compute the least common multiple of two polynomials

$f, g \in k[x_1, \ldots, x_n]$, we compute the intersection $\langle f \rangle \cap \langle g \rangle$ using our algorithm for computing the intersection of ideals. Proposition 13 assures us that this intersection is a principal ideal (in the exercises, we ask you to prove that the intersection of principal ideals is principal) and that any generator of it is a least common multiple of f and g.

This algorithm for computing least common multiples allows us to clear up a point which we left unfinished in §2: namely, the computation of the greatest common divisor of two polynomials f and g. The crucial observation is the following.

Proposition 14. *Let $f, g \in k[x_1, \ldots, x_n]$. Then*

$$\mathrm{lcm}(f, g) \cdot \mathrm{gcd}(f, g) = fg.$$

Proof. This follows by expressing f and g as products of distinct irreducibles and then using the remarks preceding Proposition 13, especially equation (1). You will provide the details in Exercise 5. □

It follows immediately from Proposition 14 that

$$\mathrm{gcd}(f, g) = \frac{f \cdot g}{\mathrm{lcm}(f, g)}. \tag{2}$$

This gives an **algorithm for computing the greatest common divisor** of two polynomials f and g. Namely, we compute $\mathrm{lcm}(f, g)$ using our algorithm for the least common multiple and divide it into the product of f and g using the division algorithm.

We should point out that the gcd algorithm just described is rather cumbersome. In practice, more efficient algorithms are used [see DAVENPORT, SIRET and TOURNIER (1993)].

Having dealt with the computation of intersections, we now ask what operation on varieties corresponds to the operation of intersection on ideals. The following result answers this question.

Theorem 15. *If I and J are ideals in $k[x_1, \ldots, x_n]$, then $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.*

Proof. Let $a \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Then $a \in \mathbf{V}(I)$ or $a \in \mathbf{V}(J)$. This means that either $f(a) = 0$ for all $f \in I$ or $f(a) = 0$ for all $f \in J$. Thus, certainly, $f(a) = 0$ for all $f \in I \cap J$. Hence, $a \in \mathbf{V}(I \cap J)$. Hence, $\mathbf{V}(I) \cup \mathbf{V}(J) \subseteq \mathbf{V}(I \cap J)$.

On the other hand, note that since $IJ \subseteq I \cap J$, we have $\mathbf{V}(I \cap J) \subseteq \mathbf{V}(IJ)$. But $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$ by Theorem 7, and we immediately obtain the reverse inequality. □

Thus, the intersection of two ideals corresponds to the same variety as the product. In view of this and the fact that the intersection is much more difficult to compute than the product, one might legitimately question the wisdom of bothering with the intersection at all. The reason is that intersection behaves much better with respect to the operation of taking radicals: the product of radical ideals need not be a radical ideal (consider IJ where $I = J$), but the intersection of radical ideals is always a radical ideal. The latter fact is a consequence of the next proposition.

Proposition 16. *If I, J are any ideals, then*

$$\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}.$$

Proof. If $f \in \sqrt{I \cap J}$, then $f^m \in I \cap J$ for some integer $m > 0$. Since $f^m \in I$, we have $f \in \sqrt{I}$. Similarly, $f \in \sqrt{J}$. Thus, $\sqrt{I \cap J} \subseteq \sqrt{I} \cap \sqrt{J}$.

For the reverse inclusion, take $f \in \sqrt{I} \cap \sqrt{J}$. Then, there exist integers $m, p > 0$ such that $f^m \in I$ and $f^p \in J$. Thus $f^{m+p} = f^m f^p \in I \cap J$, so $f \in \sqrt{I \cap J}$. □

EXERCISES FOR §3

1. Show that in $\mathbb{Q}[x, y]$, we have

$$\langle (x+y)^4(x^2+y)^2(x-5y)\rangle \cap \langle (x+y)(x^2+y)^3(x+3y)\rangle = \langle (x+y)^4(x^2+y)^3(x-5y)(x+3y)\rangle.$$

2. Prove formula (1) for the least common multiple of two polynomials f and g.
3. Prove assertion (i) of Proposition 13. In other words, show that the intersection of two principal ideals is principal.
4. Prove assertion (ii) of Proposition 13. In other words, show that the least common multiple of two polynomials f and g in $k[x_1, \ldots, x_n]$ is the generator of the ideal $\langle f \rangle \cap \langle g \rangle$.
5. Prove Proposition 14. In other words, show that the least common multiple of two polynomials times the greatest common divisor of the same two polynomials is the product of the polynomials. Hint: Use the remarks following the statement of Proposition 14.
6. Let $I_1, \ldots, I_r$ and J be ideals in $k[x_1, \ldots, x_n]$. Show the following:
   a. $(I_1 + I_2)J = I_1J + I_2J$.
   b. $(I_1 \cdots I_r)^m = I_1^m \cdots I_r^m$.
7. Let I and J be ideals in $k[x_1, \ldots, x_n]$, where k is an arbitrary field. Prove the following:
   a. If $I^\ell \subseteq J$ for some integer $\ell > 0$, then $\sqrt{I} \subseteq \sqrt{J}$.
   b. $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.
8. Let
$$f = x^4 + x^3y + x^3z^2 - x^2y^2 + x^2yz^2 - xy^3 - xy^2z^2 - y^3z^2$$
   and
$$g = x^4 + 2x^3z^2 - x^2y^2 + x^2z^4 - 2xy^2z^2 - y^2z^4.$$
   a. Use a computer algebra program to compute generators for $\langle f \rangle \cap \langle g \rangle$ and $\sqrt{\langle f \rangle \langle g \rangle}$.
   b. Use a computer algebra program to compute $\gcd(f, g)$.
   c. Let $p = x^2 + xy + xz + yz$ and $q = x^2 - xy - xz + yz$. Use a computer algebra program to calculate $\langle f, g \rangle \cap \langle p, q \rangle$.
9. For an arbitrary field, show that $\sqrt{IJ} = \sqrt{I \cap J}$. Give an example to show that the product of radical ideals need not be radical. Also give an example to show that $\sqrt{IJ}$ can differ from $\sqrt{I}\sqrt{J}$.
10. If I is an ideal in $k[x_1, \ldots, x_n]$ and $\langle f(t) \rangle$ is an ideal in $k[t]$, show that the ideal $f(t)I$ defined in the text is the product of the ideal $\tilde{I}$ generated by all elements of I in $k[x_1, \ldots, x_n, t]$ and the ideal $\langle f(t) \rangle$ generated by $f(t)$ in $k[x_1, \ldots, x_n, t]$.
11. Two ideals I and J of $k[x_1, \ldots, x_n]$ are said to be *comaximal* if and only if $I + J = k[x_1, \ldots, x_n]$.
    a. Show that if $k = \mathbb{C}$, then I and J are comaximal if and only if $\mathbf{V}(I) \cap \mathbf{V}(J) = \emptyset$. Give an example to show that this is false in general.
    b. Show that if I and J are comaximal, then $IJ = I \cap J$.

c. Is the converse to part (b) true? That is, if $IJ = I \cap J$, does it necessarily follow that I and J are comaximal? Proof or counterexample?
d. If I and J are comaximal, show that I and J^2 are comaximal. In fact, show that I^r and J^s are comaximal for all positive integers r and s.
e. Let $I_1, \ldots, I_r$ be ideals in $k[x_1, \ldots, x_n]$ and suppose that I_i and $J_i = \bigcap_{j \neq i} I_j$ are comaximal for all i. Show that

$$I_1^m \cap \cdots \cap I_r^m = (I_1 \cdots I_r)^m = (I_1 \cap \cdots \cap I_r)^m$$

for all positive integers m.

12. Let I, J be ideals in $k[x_1, \ldots, x_n]$ and suppose that $I \subseteq \sqrt{J}$. Show that $I^m \subseteq J$ for some integer $m > 0$. Hint: You will need to use the Hilbert Basis Theorem.
13. Let A be an $m \times n$ constant matrix and suppose that $x = Ay$, where we are thinking of $x \in k^m$ and $y \in k^n$ as column vectors of variables. Define a map

$$\alpha_A : k[x_1, \ldots, x_m] \longrightarrow k[y_1, \ldots, y_n]$$

by sending $f \in k[x_1, \ldots, x_m]$ to $\alpha_A(f) \in k[y_1, \ldots, y_n]$, where $\alpha_A(f)$ is the polynomial defined by $\alpha_A(f)(y) = f(Ay)$.

a. Show that α_A is k-linear, i.e., show that $\alpha_A(rf + sg) = r\alpha_A(f) + s\alpha_A(g)$ for all $r, s \in k$ and all $f, g \in k[x_1, \ldots, x_n]$.
b. Show that $\alpha_A(f \cdot g) = \alpha_A(f) \cdot \alpha_A(g)$ for all $f, g \in k[x_1, \ldots, x_n]$. (As we will see in Definition 8 of Chapter 5, §2, a map between rings which preserves addition and multiplication and also preserves the multiplicative identity is called a *ring homomorphism*. Since it is clear that $\alpha_A(1) = 1$, this shows that α_A is a ring homomorphism.)
c. Show that the set $\{f \in k[x_1, \ldots, x_m] \mid \alpha_A(f) = 0\}$ is an ideal in $k[x_1, \ldots, x_m]$. [This set is called the *kernel* of α_A and denoted $\ker(\alpha_A)$.]
d. If I is an ideal in $k[x_1, \ldots, x_n]$, show that the set $\alpha_A(I) = \{\alpha_A(f) \mid f \in I\}$ need not be an ideal in $k[y_1, \ldots, y_n]$. [We will often write $\langle \alpha_A(I) \rangle$ to denote the ideal in $k[y_1, \ldots, y_n]$ generated by the elements of $\alpha_A(I)$—it is called the *extension* of I to $k[y_1, \ldots, y_n]$.]
e. If I' is an ideal in $k[y_1, \ldots, y_n]$, set $\alpha_A^{-1}(I') = \{f \in k[x_1, \ldots, x_m] \mid \alpha_A(f) \in I'\}$. Show that $\alpha_A^{-1}(I')$ is an ideal in $k[x_1, \ldots, x_m]$ (often called the *contraction* of I').

14. Let A and α_A be as above and let $K = \ker(\alpha_A)$. Let I and J be ideals in $k[x_1, \ldots, x_m]$. Show that:

a. $I \subseteq J$ implies $\langle \alpha_A(I) \rangle \subseteq \langle \alpha_A(J) \rangle$.
b. $\langle \alpha_A(I + J) \rangle = \langle \alpha_A(I) \rangle + \langle \alpha_A(J) \rangle$.
c. $\langle \alpha_A(IJ) \rangle = \langle \alpha_A(I) \rangle \langle \alpha_A(J) \rangle$.
d. $\langle \alpha_A(I \cap J) \rangle \subseteq \langle \alpha_A(I) \rangle \cap \langle \alpha_A(J) \rangle$, with equality if $I \supseteq K$ or $J \supseteq K$ and α_A is onto.
e. $\langle \alpha_A(\sqrt{I}) \rangle \subseteq \sqrt{\langle \alpha_A(I) \rangle}$ with equality if $I \supseteq K$ and α_A is onto.

15. Let A, α_A, and $K = \ker(\alpha_A)$ be as above. Let I' and J' be ideals in $k[y_1, \ldots, y_n]$. Show that:

a. $I' \subseteq J'$ implies $\alpha_A^{-1}(I') \subseteq \alpha_A^{-1}(J')$.
b. $\alpha_A^{-1}(I' + J') \supseteq \alpha_A^{-1}(I') + \alpha_A^{-1}(J')$, with equality if α_A is onto.
c. $\alpha_A^{-1}(I'J') \supseteq (\alpha_A^{-1}(I'))(\alpha_A^{-1}(J'))$, with equality if α_A is onto and the right-hand side contains K.
d. $\alpha_A^{-1}(I' \cap J') = \alpha_A^{-1}(I') \cap \alpha_A^{-1}(J')$.
e. $\alpha_A^{-1}(\sqrt{I'}) = \sqrt{\alpha_A^{-1}(I')}$.

§4 Zariski Closures, Ideal Quotients, and Saturations

We have already encountered a number of examples of sets which are not varieties. Such sets arose very naturally in Chapter 3, where we saw that the projection of a variety need not be a variety, and in the exercises in Chapter 1, where we saw that the (set-theoretic) difference of varieties can fail to be a variety.

Whether or not a set $S \subseteq k^n$ is an affine variety, the set

$$\mathbf{I}(S) = \{f \in k[x_1, \ldots, x_n] \mid f(a) = 0 \text{ for all } a \in S\}$$

is an ideal in $k[x_1, \ldots, x_n]$ (check this!). In fact, it is radical. By the ideal–variety correspondence, $\mathbf{V}(\mathbf{I}(S))$ is a variety. The following proposition states that this variety is the smallest variety that contains the set S.

Proposition 1. *If $S \subseteq k^n$, the affine variety $\mathbf{V}(\mathbf{I}(S))$ is the smallest variety that contains S [in the sense that if $W \subseteq k^n$ is any affine variety containing S, then $\mathbf{V}(\mathbf{I}(S)) \subseteq W$].*

Proof. If $W \supseteq S$, then $\mathbf{I}(W) \subseteq \mathbf{I}(S)$ because $\mathbf{I}$ is inclusion-reversing. But then $\mathbf{V}(\mathbf{I}(W)) \supseteq \mathbf{V}(\mathbf{I}(S))$ because $\mathbf{V}$ also reverses inclusions. Since W is an affine variety, $\mathbf{V}(\mathbf{I}(W)) = W$ by Theorem 7 from §2, and the result follows. $\square$

This proposition leads to the following definition.

Definition 2. The **Zariski closure** of a subset of affine space is the smallest affine algebraic variety containing the set. If $S \subseteq k^n$, the Zariski closure of S is denoted $\overline{S}$ and is equal to $\mathbf{V}(\mathbf{I}(S))$.

We note the following properties of Zariski closure.

Lemma 3. *Let S and T be subsets of k^n. Then:*
(i) $\mathbf{I}(\overline{S}) = \mathbf{I}(S)$.
(ii) *If $S \subseteq T$, then $\overline{S} \subseteq \overline{T}$.*
(iii) $\overline{S \cup T} = \overline{S} \cup \overline{T}$.

Proof. For (i), the inclusion $\mathbf{I}(\overline{S}) \subseteq \mathbf{I}(S)$ follows from $S \subseteq \overline{S}$. Going the other way, $f \in \mathbf{I}(S)$ implies $S \subseteq \mathbf{V}(f)$. Then $S \subseteq \overline{S} \subseteq \mathbf{V}(f)$ by Definition 2, so that $f \in \mathbf{I}(\overline{S})$.

The proofs of (ii) and (iii) will be covered in the exercises. $\square$

A natural example of Zariski closure is given by elimination ideals. We can now prove the first assertion of the Closure Theorem (Theorem 3 of Chapter 3, §2).

Theorem 4 (The Closure Theorem, first part). *Assume k is algebraically closed. Let $V = \mathbf{V}(f_1, \ldots, f_s) \subseteq k^n$, and let $\pi_l : k^n \to k^{n-l}$ be projection onto the last $n - l$ coordinates. If I_l is the l-th elimination ideal $I_l = \langle f_1, \ldots, f_s\rangle \cap k[x_{l+1}, \ldots, x_n]$, then $\mathbf{V}(I_l)$ is the Zariski closure of $\pi_l(V)$.*

Proof. In view of Proposition 1, we must show that $\mathbf{V}(I_l) = \mathbf{V}(\mathbf{I}(\pi_l(V)))$. By Lemma 1 of Chapter 3, §2, we have $\pi_l(V) \subseteq \mathbf{V}(I_l)$. Since $\mathbf{V}(\mathbf{I}(\pi_l(V)))$ is the smallest variety containing $\pi_l(V)$, it follows immediately that $\mathbf{V}(\mathbf{I}(\pi_l(V))) \subseteq \mathbf{V}(I_l)$.

To get the opposite inclusion, suppose $f \in \mathbf{I}(\pi_l(V))$, i.e., $f(a_{l+1}, \ldots, a_n) = 0$ for all $(a_{l+1}, \ldots, a_n) \in \pi_l(V)$. Then, considered as an element of $k[x_1, x_2, \ldots, x_n]$, we certainly have $f(a_1, a_2, \ldots, a_n) = 0$ for all $(a_1, \ldots, a_n) \in V$. By Hilbert's Nullstellensatz, $f^N \in \langle f_1, \ldots, f_s \rangle$ for some integer N. Since f does not depend on $x_1, \ldots, x_l$, neither does f^N, and we have $f^N \in \langle f_1, \ldots, f_s \rangle \cap k[x_{l+1}, \ldots, x_n] = I_l$. Thus, $f \in \sqrt{I_l}$, which implies $\mathbf{I}(\pi_l(V)) \subseteq \sqrt{I_l}$. It follows that $\mathbf{V}(I_l) = \mathbf{V}(\sqrt{I_l}) \subseteq \mathbf{V}(\mathbf{I}(\pi_l(V)))$, and the theorem is proved. □

The conclusion of Theorem 4 can be stated as $\mathbf{V}(I_l) = \overline{\pi_l(V)}$. In general, if V is a variety, then we say that a subset $S \subseteq V$ is *Zariski dense in* V if $V = \overline{S}$, i.e., V is the Zariski closure of S. is Thus Theorem 4 tells us that $\pi_l(V)$ is Zariski dense in $\mathbf{V}(I_l)$ when the field is algebraically closed.

One context in which we encountered sets that were not varieties was in taking the difference of varieties. For example, let $V = \mathbf{V}(I)$ where $I \subseteq k[x, y, z]$ is the ideal $\langle xz, yz \rangle$ and $W = \mathbf{V}(J)$ where $J = \langle z \rangle$. Then we have already seen that V is the union of the (x, y)-plane and the z-axis. Since W is the (x, y)-plane, $V \setminus W$ is the z-axis with the origin removed [because the origin also belongs to the (x, y)-plane]. We have seen in Chapter 1 that this is not a variety. The z-axis [i.e., $\mathbf{V}(x, y)$] is the Zariski closure of $V \setminus W$.

We could ask if there is a general way to compute the ideal corresponding to the Zariski closure $\overline{V \setminus W}$ of the difference of two varieties V and W. The answer is affirmative, but it involves two new algebraic constructions on ideals called *ideal quotients* and *saturations*.

We begin with the first construction.

Definition 5. If I, J are ideals in $k[x_1, \ldots, x_n]$, then $I : J$ is the set

$$\{f \in k[x_1, \ldots, x_n] \mid fg \in I \text{ for all } g \in J\}$$

and is called the **ideal quotient** (or **colon ideal**) of I by J.

So, for example, in $k[x, y, z]$ we have

$$\begin{aligned} \langle xz, yz \rangle : \langle z \rangle &= \{f \in k[x, y, z] \mid f \cdot z \in \langle xz, yz \rangle\} \\ &= \{f \in k[x, y, z] \mid f \cdot z = Axz + Byz\} \\ &= \{f \in k[x, y, z] \mid f = Ax + By\} \\ &= \langle x, y \rangle. \end{aligned}$$

Proposition 6. *If I, J are ideals in $k[x_1, \ldots, x_n]$, then the ideal quotient $I : J$ is an ideal in $k[x_1, \ldots, x_n]$ and $I : J$ contains I.*

Proof. To show $I : J$ contains I, note that because I is an ideal, if $f \in I$, then $fg \in I$ for all $g \in k[x_1, \ldots, x_n]$ and, hence, certainly $fg \in I$ for all $g \in J$. To show that $I : J$

is an ideal, first note that $0 \in I:J$ because $0 \in I$. Let $f_1, f_2 \in I:J$. Then $f_1 g$ and $f_2 g$ are in I for all $g \in J$. Since I is an ideal $(f_1+f_2)g = f_1 g + f_2 g \in I$ for all $g \in J$. Thus, $f_1 + f_2 \in I:J$. To check closure under multiplication is equally straightforward: if $f \in I:J$ and $h \in k[x_1, \ldots, x_n]$, then $fg \in I$ and, since I is an ideal, $hfg \in I$ for all $g \in J$, which means that $hf \in I:J$. □

The algebraic properties of ideal quotients and methods for computing them will be discussed later in the section. For now, we want to explore the relation between ideal quotients and the Zariski closure of a difference of varieties.

Proposition 7.

(i) *If I and J are ideals in $k[x_1, \ldots, x_n]$, then*

$$\mathbf{V}(I) = \mathbf{V}(I + J) \cup \mathbf{V}(I:J).$$

(ii) *If V and W are varieties k^n, then*

$$V = (V \cap W) \cup (\overline{V \setminus W}).$$

(iii) *In the situation of* (i)*, we have*

$$\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} \subseteq \mathbf{V}(I:J).$$

Proof. We begin with (ii). Since V contains $V \setminus W$ and V is a variety, the smallest variety containing $V \setminus W$ must be contained in V. Hence, $\overline{V \setminus W} \subseteq V$. Since $V \cap W \subseteq V$, we have $(V \cap W) \cup (\overline{V \setminus W}) \subseteq V$.

To get the reverse containment, note that $V = (V \cap W) \cup (V \setminus W)$. Since $V \setminus W \subseteq \overline{V \setminus W}$, the desired inclusion $V \subseteq (V \cap W) \cup \overline{V \setminus W}$ follows immediately.

For (iii), we first claim that $I:J \subseteq \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$. For suppose that $f \in I:J$ and $a \in \mathbf{V}(I) \setminus \mathbf{V}(J)$. Then $fg \in I$ for all $g \in J$. Since $a \in \mathbf{V}(I)$, we have $f(a)g(a) = 0$ for all $g \in J$. Since $a \notin \mathbf{V}(J)$, there is some $g \in J$ such that $g(a) \neq 0$. Hence, $f(a) = 0$ for all $a \in \mathbf{V}(I) \setminus \mathbf{V}(J)$. Thus, $f \in \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$, which proves the claim. Since $\mathbf{V}$ reverses inclusions, we have $\mathbf{V}(I:J) \supseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$.

Finally, for (i), note that $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$ by Theorem 4 of §3. Then applying (ii) with $V = \mathbf{V}(I)$ and $W = \mathbf{V}(J)$ gives

$$\mathbf{V}(I) = \mathbf{V}(I + J) \cup \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} \subseteq \mathbf{V}(I + J) \cup \mathbf{V}(I:J),$$

where the inclusion follows from (iii). But $I \subseteq I + J$ and $I \subseteq I:J$ imply that

$$\mathbf{V}(I + J) \subseteq \mathbf{V}(I) \quad \text{and} \quad \mathbf{V}(I:J) \subseteq \mathbf{V}(I).$$

These inclusions give $\mathbf{V}(I + J) \cup \mathbf{V}(I:J) \subseteq \mathbf{V}(I)$, and then we are done. □

In Proposition 7, note that $\mathbf{V}(I + J)$ from part (i) matches up with $V \cap W$ in part (ii) since $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$. So it is natural to ask if $\mathbf{V}(I:J)$ in part (i) matches up with $\overline{V \setminus W}$ in part (ii). This is equivalent to asking if the inclusion $\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} \subseteq \mathbf{V}(I:J)$ in part (iii) is an equality.

Unfortunately, this can fail, even when the field is algebraically closed. To see what can go wrong, let $I = \langle x^2(y-1)\rangle$ and $J = \langle x\rangle$ in the polynomial ring $\mathbb{C}[x,y]$. Then one easily checks that

$$\mathbf{V}(I) = \mathbf{V}(x) \cup \mathbf{V}(y-1) = \mathbf{V}(J) \cup \mathbf{V}(y-1) \subseteq \mathbb{C}^2,$$

which is the union of the y-axis and the line $y = 1$. It follows without difficulty that $\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} = \mathbf{V}(y-1)$. However, the ideal quotient is

$$\begin{aligned} I : J = \langle x^2(y-1)\rangle : \langle x\rangle &= \{f \in \mathbb{C}[x,y] \mid f \cdot x = Ax^2(y-1)\} \\ &= \{f \in \mathbb{C}[x,y] \mid f = Ax(y-1)\} = \langle x(y-1)\rangle. \end{aligned}$$

Then $\mathbf{V}(I : J) = \mathbf{V}(x(y-1)) = \mathbf{V}(x) \cup \mathbf{V}(y-1)$, which is strictly bigger than $\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} = \mathbf{V}(y-1)$. In other words, the inclusion in part (iii) of Proposition 7 can be strict, even over an algebraically closed field.

However, if we replace J with J^2, then a computation similar to the above gives $I : J^2 = \langle y-1\rangle$, so that $\mathbf{V}(I : J^2) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$. In general, higher powers may be required, which leads to our second algebraic construction on ideals.

Definition 8. If I, J are ideals in $k[x_1,\dots,x_n]$, then $I : J^\infty$ is the set

$$\{f \in k[x_1,\dots,x_n] \mid \text{for all } g \in J, \text{ there is } N \geq 0 \text{ such that } fg^N \in I\}$$

and is called the **saturation** of I with respect to J.

Proposition 9. *If I, J are ideals in $k[x_1,\dots,x_n]$, then the saturation $I : J^\infty$ is an ideal in $k[x_1,\dots,x_n]$. Furthermore:*
(i) $I \subseteq I : J \subseteq I : J^\infty$.
(ii) $I : J^\infty = I : J^N$ *for all sufficiently large N.*
(iii) $\sqrt{I : J^\infty} = \sqrt{I} : J$.

Proof. First observe that $J_1 \subseteq J_2$ implies $I : J_2 \subseteq I : J_1$. Since $J^{N+1} \subseteq J^N$ for all N, we obtain the ascending chain of ideals

$$I \subseteq I : J \subseteq I : J^2 \subseteq I : J^3 \subseteq \cdots. \tag{1}$$

By the ACC, there is N such that $I : J^N = I : J^{N+1} = \cdots$. We claim that $I : J^\infty = I : J^N$. One inclusion is easy, for if $f \in I : J^N$ and $g \in J$, then $g^N \in J^N$. Hence, $fg^N \in I$, proving that $f \in I : J^\infty$. For the other inclusion, take $f \in I : J^\infty$ and let $J = \langle g_1,\dots,g_s\rangle$. By Definition 8, f times a power of g_i lies in I. If M is the largest such power, then $fg_i^M \in I$ for $i = 1,\dots,s$. In the exercises, you will show that

$$J^{sM} \subseteq \langle g_1^M,\dots,g_s^M\rangle.$$

This implies $fJ^{sM} \subseteq I$, so that $f \in I : J^{sM}$. Then $f \in I : J^N$ since (1) stabilizes at N.

Part (ii) follows from the claim just proved, and $I : J^\infty = I : J^N$ implies that $I : J^\infty$ is an ideal by Proposition 6. Note also that part (i) follows from (1) and part (ii) .

For part (iii), we first show $\sqrt{I:J^\infty} \subseteq \sqrt{I}:J$. This is easy, for $f \in \sqrt{I:J^\infty}$ implies $f^m \in I:J^\infty$ for some m. Given $g \in J$, it follows that $f^m g^N \in I$ for some N. Then $(fg)^M \in I$ for $M = \max(m, N)$, so that $fg \in \sqrt{I}$. Since this holds for all $g \in J$, we conclude that $f \in \sqrt{I}:J$.

For the opposite inclusion, take $f \in \sqrt{I}:J$ and write $J = \langle g_1, \dots, g_s \rangle$. Then $fg_i \in \sqrt{I}$, so we can find M with $f^M g_i^M \in I$ for all i. The argument from (ii) implies $f^M J^{sM} \subseteq I$, so

$$f^M \in I:J^{sM} \subseteq I:J^\infty.$$

It follows that $f \in \sqrt{I:J^\infty}$, and the proof is complete. □

Later in the section we will discuss further algebraic properties of saturations and how to compute them. For now, we focus on their relation to geometry.

Theorem 10. *Let I and J be ideals in $k[x_1, \dots, x_n]$. Then:*
(i) $\mathbf{V}(I) = \mathbf{V}(I + J) \cup \mathbf{V}(I:J^\infty)$.
(ii) $\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)} \subseteq \mathbf{V}(I:J^\infty)$.
(iii) *If k is algebraically closed, then* $\mathbf{V}(I:J^\infty) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$.

Proof. In the exercises, you will show that (i) and (ii) follow by easy modifications of the proofs of parts (i) and (iii) of Proposition 7.

For (iii), suppose that k is algebraically closed. We first show that

$$\mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J)) \subseteq \sqrt{I}:J. \tag{2}$$

Let $f \in \mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))$. If $g \in J$, then fg vanishes on $\mathbf{V}(I)$ because f vanishes on $\mathbf{V}(I) \setminus \mathbf{V}(J)$ and g on $\mathbf{V}(J)$. Thus, $fg \in \mathbf{I}(\mathbf{V}(I))$, so $fg \in \sqrt{I}$ by the Nullstellensatz. Since this holds for all $g \in J$, we have $f \in \sqrt{I}:J$, as claimed.

Since $\mathbf{V}$ is inclusion-reversing, (2) implies

$$\mathbf{V}(\sqrt{I}:J) \subseteq \mathbf{V}(\mathbf{I}(\mathbf{V}(I) \setminus \mathbf{V}(J))) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}.$$

However, we also have

$$\mathbf{V}(I:J^\infty) = \mathbf{V}(\sqrt{I:J^\infty}) = \mathbf{V}(\sqrt{I}:J),$$

where the second equality follows from part (iii) of Proposition 9. Combining the last two displays, we obtain

$$\mathbf{V}(I:J^\infty) \subseteq \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}.$$

Then (iii) follows immediately from this inclusion and (ii). □

When k is algebraically closed, Theorem 10 and Theorem 4 of §3 imply that the decomposition

$$\mathbf{V}(I) = \mathbf{V}(I + J) \cup \mathbf{V}(I:J^\infty)$$

is *precisely* the decomposition

$$\mathbf{V}(I) = (\mathbf{V}(I) \cap \mathbf{V}(J)) \cup (\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)})$$

from part (ii) of Proposition 7. This shows that the saturation $I : J^\infty$ is the ideal-theoretic analog of the Zariski closure $\overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}$.

In some situations, saturations can be replaced with ideal quotients. For example, the proof of Theorem 10 yields the following corollary when the ideal I is radical.

Corollary 11. *Let I and J be ideals in $k[x_1, \ldots, x_n]$. If k is algebraically closed and I is radical, then*

$$\mathbf{V}(I : J) = \overline{\mathbf{V}(I) \setminus \mathbf{V}(J)}.$$

You will prove this in the exercises. Another nice fact (also covered in the exercises) is that if k is arbitrary and V and W are varieties in k^n, then

$$\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V \setminus W).$$

The following proposition takes care of some simple properties of ideal quotients and saturations.

Proposition 12. *Let I and J be ideals in $k[x_1, \ldots, x_n]$. Then:*

(i) $I : k[x_1, \ldots, x_n] = I : k[x_1, \ldots, x_n]^\infty = I$.
(ii) $J \subseteq I$ *if and only if* $I : J = k[x_1, \ldots, x_n]$.
(iii) $J \subseteq \sqrt{I}$ *if and only if* $I : J^\infty = k[x_1, \ldots, x_n]$.

Proof. The proof is left as an exercise. □

When the field is algebraically closed, the reader is urged to translate parts (i) and (iii) of the proposition into terms of varieties (upon which they become clear).

The following proposition will help us compute ideal quotients and saturations.

Proposition 13. *Let I and $J_1, \ldots, J_r$ be ideals in $k[x_1, \ldots, x_n]$. Then:*

$$I : \Big(\sum_{i=1}^r J_i\Big) = \bigcap_{i=1}^r \big(I : J_i\big), \tag{3}$$

$$I : \Big(\sum_{i=1}^r J_i\Big)^\infty = \bigcap_{i=1}^r \big(I : J_i^\infty\big). \tag{4}$$

Proof. We again leave the (straightforward) proofs to the reader. □

If f is a polynomial and I an ideal, we will often write $I : f$ instead of $I : \langle f \rangle$, and similarly $I : f^\infty$ instead of $I : \langle f \rangle^\infty$. Note that (3) and (4) imply that

$$I : \langle f_1, f_2, \ldots, f_r \rangle = \bigcap_{i=1}^r (I : f_i) \ \text{ and } \ I : \langle f_1, f_2, \ldots, f_r \rangle^\infty = \bigcap_{i=1}^r (I : f_i^\infty). \tag{5}$$

We now turn to the question of how to compute generators of the ideal quotient $I : J$ and saturation $I : J^\infty$, given generators of I and J. Inspired by (5), we begin with the case when J is generated by a single polynomial.

Theorem 14. *Let I be an ideal and g an element of $k[x_1,\ldots,x_n]$. Then:*

(i) *If $\{h_1,\ldots,h_p\}$ is a basis of the ideal $I \cap \langle g\rangle$, then $\{h_1/g,\ldots,h_p/g\}$ is a basis of $I:g$.*

(ii) *If $\{f_1,\ldots,f_s\}$ is a basis of I and $\tilde{I} = \langle f_1,\ldots,f_s, 1-yg\rangle \subseteq k[x_1,\ldots,x_n,y]$, where y is a new variable, then*

$$I:g^\infty = \tilde{I} \cap k[x_1,\ldots,x_n].$$

Furthermore, if G is a lex Gröbner basis of $\tilde{I}$ for $y > x_1 > \cdots > x_n$, then $G \cap k[x_1,\ldots,x_n]$ is a basis of $I:g^\infty$.

Proof. For (i), observe that if $h \in \langle g\rangle$, then $h = bg$ for some polynomial $b \in k[x_1,\ldots,x_n]$. Thus, if $f \in \langle h_1/g,\ldots,h_p/g\rangle$, then

$$hf = bgf \in \langle h_1,\ldots,h_p\rangle = I \cap \langle g\rangle \subseteq I.$$

Thus, $f \in I:g$. Conversely, suppose $f \in I:g$. Then $fg \in I$. Since $fg \in \langle g\rangle$, we have $fg \in I \cap \langle g\rangle$. If $I \cap \langle g\rangle = \langle h_1,\ldots,h_p\rangle$, this means $fg = \sum r_i h_i$ for some polynomials r_i. Since each $h_i \in \langle g\rangle$, each h_i/g is a polynomial, and we conclude that $f = \sum r_i(h_i/g)$, whence $f \in \langle h_1/g,\ldots,h_p/g\rangle$.

The first assertion of (ii) is left as an exercise. Then the Elimination Theorem from Chapter 3, §1 implies that $G \cap k[x_1,\ldots,x_n]$ is a Gröbner basis of $I:g^\infty$. □

This theorem, together with our procedure for computing intersections of ideals and equation (5), immediately leads to an **algorithm for computing a basis of an ideal quotient**: given $I = \langle f_1,\ldots,f_r\rangle$ and $J = \langle g_1,\ldots,g_s\rangle$, to compute a basis of $I:J$, we first compute a basis for $I:g_i$ for each i. In view of Theorem 14, this means computing a basis $\{h_1,\ldots,h_p\}$ of $\langle f_1,\ldots,f_r\rangle \cap \langle g_i\rangle$. Recall that we do this via the algorithm for computing intersections of ideals from §3. Using the division algorithm, we divide each of basis element h_j by g_i to get a basis for $I:g_i$ by part (i) of Theorem 14. Finally, we compute a basis for $I:J$ by applying the intersection algorithm $s-1$ times, computing first a basis for $I:\langle g_1,g_2\rangle = (I:g_1)\cap(I:g_2)$, then a basis for $I:\langle g_1,g_2,g_3\rangle = (I:\langle g_1,g_2\rangle)\cap(I:g_3)$, and so on.

Similarly, we have an **algorithm for computing a basis of a saturation**: given $I = \langle f_1,\ldots,f_r\rangle$ and $J = \langle g_1,\ldots,g_s\rangle$, to compute a basis of $I:J^\infty$, we first compute a basis for $I:g_i^\infty$ for each i using the method described in part (ii) of Theorem 14. Then by (5), we need to intersect the ideals $I:g_i^\infty$, which we do as above by applying the intersection algorithm $s-1$ times.

EXERCISES FOR §4

1. Find the Zariski closure of the following sets:
   a. The projection of the hyperbola $\mathbf{V}(xy-1)$ in $\mathbb{R}^2$ onto the x-axis.
   b. The boundary of the first quadrant in $\mathbb{R}^2$.
   c. The set $\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2 \le 4\}$.
2. Complete the proof of Lemma 3. Hint: For part (iii), use Lemma 2 from Chapter 1, §2.
3. Let $f = (x+y)^2(x-y)(x+z^2)$ and $g = (x+z^2)^3(x-y)(z+y)$. Compute generators for $\langle f\rangle : \langle g\rangle$.

4. Let I and J be ideals in $k[x_1, \ldots, x_n]$. Show that if I is radical, then $I : J$ is radical and $I : J = I : \sqrt{J} = I : J^\infty$.
5. As in the proof of Proposition 9, assume $J = \langle g_1, \ldots, g_s \rangle$. Prove that $J^{sM} \subseteq \langle g_1^M, \ldots, g_s^M \rangle$. Hint: See the proof of Lemma 5 of §2.
6. Prove parts (i) and (ii) of Theorem 10. Hint: Adapt the proofs of parts (i) and (iii) of Proposition 7.
7. Prove Corollary 11. Hint: Combine Theorem 10 and the Exercise 4. Another approach would be look closely at the proof of Theorem 10 when I is radical.
8. Let $V, W \subseteq k^n$ be varieties. Prove that $\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V \setminus W)$.
9. Prove Proposition 12 and find geometric interpretations of parts (i) and (iii)
10. Prove Proposition 13 and find a geometric interpretation of (4).
11. Prove $I : g^\infty = \tilde{I} \cap k[x_1, \ldots, x_n]$ from part (ii) of Theorem 14. Hint: See the proof of Proposition 8 of §2.
12. Show that Proposition 8 of §2 is a corollary of Proposition 12 and Theorem 14.
13. An example mentioned in the text used $I = \langle x^2(y-1) \rangle$ and $J = \langle x \rangle$. Compute $I : J^\infty$ and explain how your answer relates to the discussion in the text.
14. Let $I, J \subseteq k[x_1, \ldots, x_n]$ be ideals. Prove that $I : J^\infty = I : J^N$ if and only if $I : J^N = I : J^{N+1}$. Then use this to describe an algorithm for computing the saturation $I : J^\infty$ based on the algorithm for computing ideal quotients.
15. Show that N can be arbitrarily large in $I : J^\infty = I : J^N$. Hint: Look at $I = \langle x^N(y-1) \rangle$.
16. Let $I, J, K \subseteq k[x_1, \ldots, x_n]$ be ideals. Prove the following:
    a. $IJ \subseteq K$ if and only if $I \subseteq K : J$.
    b. $(I : J) : K = I : JK$.
17. Given ideals $I_1, \ldots, I_r, J \subseteq k[x_1, \ldots, x_n]$, prove that $\left(\bigcap_{i=1}^r I_i\right) : J = \bigcap_{i=1}^r (I_i : J)$. Then prove a similar result for saturations and give a geometric interpretation.
18. Let A be an $m \times n$ constant matrix and suppose that $x = Ay$. where we are thinking of $x \in k^m$ and $y \in k^n$ as column vectors of variables. As in Exercise 13 of §3, define a map
$$\alpha_A : k[x_1, \ldots, x_m] \longrightarrow k[y_1, \ldots, y_n]$$
    by sending $f \in k[x_1, \ldots, x_m]$ to $\alpha_A(f) \in k[y_1, \ldots, y_n]$, where $\alpha_A(f)$ is the polynomial defined by $\alpha_A(f)(y) = f(Ay)$.
    a. Show that $\alpha_A(I : J) \subseteq \alpha_A(I) : \alpha_A(J)$ with equality if $I \supseteq \ker(\alpha_A)$ and α_A is onto.
    b. Show that $\alpha_A^{-1}(I' : J') = \alpha_A^{-1}(I') : \alpha_A^{-1}(J')$ when α_A is onto.

§5 Irreducible Varieties and Prime Ideals

We have already seen that the union of two varieties is a variety. For example, in Chapter 1 and in the last section, we considered $\mathbf{V}(xz, yz)$, which is the union of a line and a plane. Intuitively, it is natural to think of the line and the plane as "more fundamental" than $\mathbf{V}(xz, yz)$. Intuition also tells us that a line or a plane are "irreducible" or "indecomposable" in some sense: they do not obviously seem to be a union of finitely many simpler varieties. We formalize this notion as follows.

Definition 1. An affine variety $V \subseteq k^n$ is **irreducible** if whenever V is written in the form $V = V_1 \cup V_2$, where V_1 and V_2 are affine varieties, then either $V_1 = V$ or $V_2 = V$.

Thus, $\mathbf{V}(xz, yz)$ is not an irreducible variety. On the other hand, it is not completely clear when a variety is irreducible. If this definition is to correspond to our geometric intuition, it is clear that a point, a line, and a plane ought to be irreducible. For that matter, the twisted cubic $\mathbf{V}(y - x^2, z - x^3)$ in $\mathbb{R}^3$ appears to be irreducible. But how do we prove this? The key is to capture this notion algebraically: if we can characterize ideals which correspond to irreducible varieties, then perhaps we stand a chance of establishing whether a variety is irreducible.

The following notion turns out to be the right one.

Definition 2. An ideal $I \subseteq k[x_1, \ldots, x_n]$ is **prime** if whenever $f, g \in k[x_1, \ldots, x_n]$ and $fg \in I$, then either $f \in I$ or $g \in I$.

If we have set things up right, an irreducible variety will correspond to a prime ideal and conversely. The following theorem assures us that this is indeed the case.

Proposition 3. *Let $V \subseteq k^n$ be an affine variety. Then V is irreducible if and only if $\mathbf{I}(V)$ is a prime ideal.*

Proof. First, assume that V is irreducible and let $fg \in \mathbf{I}(V)$. Set $V_1 = V \cap \mathbf{V}(f)$ and $V_2 = V \cap \mathbf{V}(g)$; these are affine varieties because an intersection of affine varieties is a variety. Then $fg \in \mathbf{I}(V)$ easily implies that $V = V_1 \cup V_2$. Since V is irreducible, we have either $V = V_1$ or $V = V_2$. Say the former holds, so that $V = V_1 = V \cap \mathbf{V}(f)$. This implies that f vanishes on V, so that $f \in \mathbf{I}(V)$. Thus, $\mathbf{I}(V)$ is prime.

Next, assume that $\mathbf{I}(V)$ is prime and let $V = V_1 \cup V_2$. Suppose that $V \neq V_1$. We claim that $\mathbf{I}(V) = \mathbf{I}(V_2)$. To prove this, note that $\mathbf{I}(V) \subseteq \mathbf{I}(V_2)$ since $V_2 \subseteq V$. For the opposite inclusion, first note that $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$ since $V_1 \subsetneq V$. Thus, we can pick $f \in \mathbf{I}(V_1) \setminus \mathbf{I}(V)$. Now take any $g \in \mathbf{I}(V_2)$. Since $V = V_1 \cup V_2$, it follows that fg vanishes on V, and, hence, $fg \in \mathbf{I}(V)$. But $\mathbf{I}(V)$ is prime, so that f or g lies in $\mathbf{I}(V)$. We know that $f \notin \mathbf{I}(V)$ and, thus, $g \in \mathbf{I}(V)$. This proves $\mathbf{I}(V) = \mathbf{I}(V_2)$, whence $V = V_2$ because $\mathbf{I}$ is one-to-one. Thus, V is an irreducible variety. $\square$

It is an easy exercise to show that every prime ideal is radical. Then, using the ideal-variety correspondence between radical ideals and varieties, we get the following corollary of Proposition 3.

Corollary 4. *When k is algebraically closed, the functions* $\mathbf{I}$ *and* $\mathbf{V}$ *induce a one-to-one correspondence between irreducible varieties in k^n and prime ideals in $k[x_1, \ldots, x_n]$.*

As an example of how to use Proposition 3, let us prove that the ideal $\mathbf{I}(V)$ of the twisted cubic is prime. Suppose that $fg \in \mathbf{I}(V)$. Since the curve is parametrized by (t, t^2, t^3), it follows that, for all t,

$$f(t, t^2, t^3)g(t, t^2, t^3) = 0.$$

This implies that $f(t, t^2, t^3)$ or $g(t, t^2, t^3)$ must be the zero polynomial, so that f or g vanishes on V. Hence, f or g lies in $\mathbf{I}(V)$, proving that $\mathbf{I}(V)$ is a prime ideal.

By the proposition, the twisted cubic is an irreducible variety in $\mathbb{R}^3$. One proves that a straight line is irreducible in the same way: first parametrize it, then apply the above argument.

In fact, the above argument holds much more generally.

Proposition 5. *If k is an infinite field and $V \subseteq k^n$ is a variety defined parametrically*

$$\begin{aligned} x_1 &= f_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= f_n(t_1, \ldots, t_m), \end{aligned}$$

where $f_1, \ldots, f_n$ are polynomials in $k[t_1, \ldots, t_m]$, then V is irreducible.

Proof. As in §3 of Chapter 3, we let $F : k^m \to k^n$ be defined by

$$F(t_1, \ldots, t_m) = (f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Saying that V is defined parametrically by the above equations means that V is the Zariski closure of $F(k^m)$. In particular, $\mathbf{I}(V) = \mathbf{I}(F(k^m))$.

For any polynomial $g \in k[x_1, \ldots, x_n]$, the function $g \circ F$ is a polynomial in $k[t_1, \ldots, t_m]$. In fact, $g \circ F$ is the polynomial obtained by "plugging the polynomials $f_1, \ldots, f_n$ into g":

$$g \circ F = g(f_1(t_1, \ldots, t_m), \ldots, f_n(t_1, \ldots, t_m)).$$

Because k is infinite, $\mathbf{I}(V) = \mathbf{I}(F(k^m))$ is the set of polynomials in $k[x_1, \ldots, x_n]$ whose composition with F is the zero polynomial in $k[t_1, \ldots, t_m]$:

$$\mathbf{I}(V) = \{g \in k[x_1, \ldots, x_n] \mid g \circ F = 0\}.$$

Now suppose that $gh \in \mathbf{I}(V)$. Then $(gh) \circ F = (g \circ F)(h \circ F) = 0$. (Make sure you understand this.) But, if the product of two polynomials in $k[t_1, \ldots, t_m]$ is the zero polynomial, one of them must be the zero polynomial. Hence, either $g \circ F = 0$ or $h \circ F = 0$. This means that either $g \in \mathbf{I}(V)$ or $h \in \mathbf{I}(V)$. This shows that $\mathbf{I}(V)$ is a prime ideal and, therefore, that V is irreducible. $\square$

With a little care, the above argument extends still further to show that any variety defined by a *rational* parametrization is irreducible.

Proposition 6. *If k is an infinite field and V is a variety defined by the rational parametrization*

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}, \end{aligned}$$

where $f_1, \ldots, f_n, g_1, \ldots, g_n \in k[t_1, \ldots, t_m]$, then V is irreducible.

Proof. Set $W = \mathbf{V}(g_1 g_2 \cdots g_n)$ and let $F : k^m \setminus W \to k^n$ defined by

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_n, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right).$$

Then V is the Zariski closure of $F(k^m \setminus W)$, which implies that $\mathbf{I}(V)$ is the set of $h \in k[x_1, \ldots, x_n]$ such that the function $h \circ F$ is zero for all $(t_1, \ldots, t_m) \in k^m \setminus W$. The difficulty is that $h \circ F$ need not be a polynomial, and we, thus, cannot directly apply the argument in the latter part of the proof of Proposition 5.

We can get around this difficulty as follows. Let $h \in k[x_1, \ldots, x_n]$. Since

$$g_1(t_1, \ldots, t_m) g_2(t_1, \ldots, t_m) \cdots g_n(t_1, \ldots, t_m) \neq 0$$

for any $(t_1, \ldots, t_m) \in k^m \setminus W$, the function $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is equal to zero at precisely those values of $(t_1, \ldots, t_m) \in k^m \setminus W$ for which $h \circ F$ is equal to zero. Moreover, if we let N be the total degree of $h \in k[x_1, \ldots, x_n]$, then we leave it as an exercise to show that $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is a polynomial in $k[t_1, \ldots, t_m]$. We deduce that $h \in \mathbf{I}(V)$ if and only if $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is zero for all $t \in k^m \setminus W$. But, by Exercise 11 of Chapter 3, §3, this happens if and only if $(g_1 g_2 \cdots g_n)^N (h \circ F)$ is the zero polynomial in $k[t_1, \ldots, t_m]$. Thus, we have shown that

$$h \in \mathbf{I}(V) \quad \text{if and only if} \quad (g_1 g_2 \cdots g_n)^N (h \circ F) = 0 \in k[t_1, \ldots, t_m].$$

Now, we continue our proof that $\mathbf{I}(V)$ is prime. Suppose $p, q \in k[x_1, \ldots, x_n]$ satisfy $p \cdot q \in \mathbf{I}(V)$. If the total degrees of p and q are M and N, respectively, then the total degree of $p \cdot q$ is $M + N$. Thus, $(g_1 g_2 \cdots g_n)^{M+N} (p \circ F) \cdot (q \circ F) = 0$. But the former is a product of the polynomials $(g_1 g_2 \cdots g_n)^M (p \circ F)$ and $(g_1 g_2 \cdots g_n)^N (q \circ F)$ in $k[t_1, \ldots, t_m]$. Hence one of them must be the zero polynomial. In particular, either $p \in \mathbf{I}(V)$ or $q \in \mathbf{I}(V)$. This shows that $\mathbf{I}(V)$ is a prime ideal and, therefore, that V is an irreducible variety. □

The simplest variety in k^n given by a parametrization consists of a single point, $\{(a_1, \ldots, a_n)\}$. In the notation of Proposition 5, it is given by the parametrization in which each f_i is the constant polynomial $f_i(t_1, \ldots, t_m) = a_i$, $1 \leq i \leq n$. It is clearly irreducible and it is easy to check that $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ (see Exercise 7), which implies that the latter is prime. The ideal $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ has another distinctive property: it is maximal in the sense that the only ideal which strictly contains it is the whole ring $k[x_1, \ldots, x_n]$. Such ideals are important enough to merit special attention.

Definition 7. An ideal $I \subseteq k[x_1, \ldots, x_n]$ is said to be **maximal** if $I \neq k[x_1, \ldots, x_n]$ and any ideal J containing I is such that either $J = I$ or $J = k[x_1, \ldots, x_n]$.

In order to streamline statements, we make the following definition.

Definition 8. An ideal $I \subseteq k[x_1, \ldots, x_n]$ is said to be **proper** if I is not equal to $k[x_1, \ldots, x_n]$.

Thus, an ideal is maximal if it is proper and no other proper ideal strictly contains it. We now show that any ideal of the form $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ is maximal.

Proposition 9. *If k is any field, an ideal $I \subseteq k[x_1, \ldots, x_n]$ of the form*

$$I = \langle x_1 - a_1, \ldots, x_n - a_n\rangle,$$

where $a_1, \ldots, a_n \in k$, is maximal.

Proof. Suppose that J is some ideal strictly containing I. Then there must exist $f \in J$ such that $f \notin I$. We can use the division algorithm to write f as $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) + b$ for some $b \in k$. Since $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) \in I$ and $f \notin I$, we must have $b \neq 0$. However, since $f \in J$ and since $A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n) \in I \subseteq J$, we also have

$$b = f - (A_1(x_1 - a_1) + \cdots + A_n(x_n - a_n)) \in J.$$

Since b is nonzero, $1 = 1/b \cdot b \in J$, so $J = k[x_1, \ldots, x_n]$. $\square$

Since

$$\mathbf{V}(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\},$$

every point $(a_1, \ldots, a_n) \in k^n$ corresponds to a maximal ideal of $k[x_1, \ldots, x_n]$, namely $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$. The converse does not hold if k is not algebraically closed. In the exercises, we ask you to show that $\langle x^2 + 1\rangle$ is maximal in $\mathbb{R}[x]$. The latter does not correspond to a point of $\mathbb{R}$. The following result, however, holds in any polynomial ring.

Proposition 10. *If k is any field, a maximal ideal in $k[x_1, \ldots, x_n]$ is prime.*

Proof. Suppose that I is a proper ideal which is not prime and let $fg \in I$, where $f \notin I$ and $g \notin I$. Consider the ideal $\langle f\rangle + I$. This ideal strictly contains I because $f \notin I$. Moreover, if we were to have $\langle f\rangle + I = k[x_1, \ldots, x_n]$, then $1 = cf + h$ for some polynomial c and some $h \in I$. Multiplying through by g would give $g = cfg + hg \in I$ which would contradict our choice of g. Thus, $I + \langle f\rangle$ is a proper ideal containing I, so that I is not maximal. $\square$

Note that Propositions 9 and 10 together imply that $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ is prime in $k[x_1, \ldots, x_n]$ even if k is not infinite. Over an algebraically closed field, it turns out that every maximal ideal corresponds to some point of k^n.

Theorem 11. *If k is an algebraically closed field, then every maximal ideal of $k[x_1, \ldots, x_n]$ is of the form $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ for some $a_1, \ldots, a_n \in k$.*

Proof. Let $I \subseteq k[x_1, \ldots, x_n]$ be maximal. Since $I \neq k[x_1, \ldots, x_n]$, we have $\mathbf{V}(I) \neq \emptyset$ by the Weak Nullstellensatz (Theorem 1 of §1). Hence, there is some point $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. This means that every $f \in I$ vanishes at $(a_1, \ldots, a_n)$, so that $f \in \mathbf{I}(\{(a_1, \ldots, a_n)\})$. Thus, we can write

$$I \subseteq \mathbf{I}(\{(a_1, \ldots, a_n)\}).$$

We have already observed that $\mathbf{I}(\{(a_1, \ldots, a_n)\}) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ (see Exercise 7), and, thus, the above inclusion becomes

$$I \subseteq \langle x_1 - a_1, \ldots, x_n - a_n \rangle \subsetneq k[x_1, \ldots, x_n].$$

Since I is maximal, it follows that $I = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. □

Note the proof of Theorem 11 uses the Weak Nullstellensatz. It is not difficult to see that it is, in fact, equivalent to the Weak Nullstellensatz.

We have the following easy corollary of Theorem 11.

Corollary 12. *If k is an algebraically closed field, then there is a one-to-one correspondence between points of k^n and maximal ideals of $k[x_1, \ldots, x_n]$.*

Thus, we have extended our algebra–geometry dictionary. Over an algebraically closed field, every nonempty irreducible variety corresponds to a proper prime ideal, and conversely. Every point corresponds to a maximal ideal, and conversely.

We can use Zariski closure to characterize when a variety is irreducible.

Proposition 13. *A variety V is irreducible if and only if for every variety $W \subsetneq V$, the difference $V \setminus W$ is Zariski dense in V.*

Proof. First assume that V is irreducible and take $W \subsetneq V$. Then Proposition 7 of §4 gives the decomposition $V = W \cup \overline{V \setminus W}$. Since V is irreducible and $V \neq W$, this forces $V = \overline{V \setminus W}$.

For the converse, suppose that $V = V_1 \cup V_2$. If $V_1 \subsetneq V$, then $\overline{V \setminus V_1} = V$. But $V \setminus V_1 \subseteq V_2$, so that $\overline{V \setminus V_1} \subseteq V_2$. This implies $V \subseteq V_2$, and $V = V_2$ follows. □

Let us make a final comment about terminology. Some references, such as HARTSHORNE (1977), use the term "variety" for what we call an irreducible variety and say "algebraic set" instead of variety. When reading other books on algebraic geometry, be sure to check the definitions!

EXERCISES FOR §5

1. If $h \in k[x_1, \ldots, x_n]$ has total degree N and if F is as in Proposition 6, show that $(g_1 g_2 \ldots g_n)^N (h \circ F)$ is a polynomial in $k[t_1, \ldots, t_m]$.
2. Show that a prime ideal is radical.
3. Show that an ideal I is prime if and only if for any ideals J and K such that $JK \subseteq I$, either $J \subseteq I$ or $K \subseteq I$.
4. Let $I_1, \ldots, I_n$ be ideals and P a prime ideal containing $\bigcap_{i=1}^n I_i$. Then prove that $P \supseteq I_i$ for some i. Further, if $P = \bigcap_{i=1}^n I_i$, show that $P = I_i$ for some i.
5. Express $f = x^2z - 6y^4 + 2xy^3z$ in the form $f = f_1(x, y, z)(x + 3) + f_2(x, y, z)(y - 1) + f_3(x, y, z)(z - 2)$ for some $f_1, f_2, f_3 \in k[x, y, z]$.

6. Let k be an infinite field.
   a. Show that any straight line in k^n is irreducible.
   b. Prove that any linear subspace of k^n is irreducible. Hint: Parametrize and use Proposition 5.
7. Show that
$$\mathbf{I}(\{(a_1,\ldots,a_n)\}) = \langle x_1 - a_1,\ldots,x_n - a_n\rangle.$$
8. Show the following:
   a. $\langle x^2 + 1\rangle$ is maximal in $\mathbb{R}[x]$.
   b. If $I \subseteq \mathbb{R}[x_1,\ldots,x_n]$ is maximal, show that $\mathbf{V}(I)$ is either empty or a point in $\mathbb{R}^n$. Hint: Examine the proof of Theorem 11.
   c. Give an example of a maximal ideal I in $\mathbb{R}[x_1,\ldots,x_n]$ for which $\mathbf{V}(I) = \emptyset$. Hint: Consider the ideal $\langle x_1^2 + 1, x_2,\ldots,x_n\rangle$.
9. Suppose that k is a field which is not algebraically closed.
   a. Show that if $I \subseteq k[x_1,\ldots,x_n]$ is maximal, then $\mathbf{V}(I)$ is either empty or a point in k^n. Hint: Examine the proof of Theorem 11.
   b. Show that there exists a maximal ideal I in $k[x_1,\ldots,x_n]$ for which $\mathbf{V}(I) = \emptyset$. Hint: See the previous exercise.
   c. Conclude that if k is not algebraically closed, there is always a maximal ideal of $k[x_1,\ldots,x_n]$ which is not of the form $\langle x_1 - a_1,\ldots,x_n - a_n\rangle$.
10. Prove that Theorem 11 implies the Weak Nullstellensatz.
11. If $f \in \mathbb{C}[x_1,\ldots,x_n]$ is irreducible, then $\mathbf{V}(f)$ is irreducible. Hint: Show that $\langle f\rangle$ is prime.
12. Prove that if I is any proper ideal in $\mathbb{C}[x_1,\ldots,x_n]$, then $\sqrt{I}$ is the intersection of all maximal ideals containing I. Hint: Use Theorem 11.
13. Let $f_1,\ldots,f_n \in k[x_1]$ be polynomials of one variable and consider the ideal
$$I = \langle f_1(x_1), x_2 - f_2(x_1),\ldots,x_n - f_n(x_1)\rangle \subseteq k[x_1,\ldots,x_n].$$
   We also assume that $\deg(f_1) = m > 0$.
   a. Show that every $f \in k[x_1,\ldots,x_n]$ can be written uniquely as $f = q + r$ where $q \in I$ and $r \in k[x_1]$ with either $r = 0$ or $\deg(r) < m$. Hint: Use lex order with x_1 last.
   b. Let $f \in k[x_1]$. Use part (a) to show that $f \in I$ if and only if f is divisible by f_1 in $k[x_1]$.
   c. Prove that I is prime if and only if $f_1 \in k[x_1]$ is irreducible.
   d. Prove that I is radical if and only if $f_1 \in k[x_1]$ is square-free.
   e. Prove that $\sqrt{I} = \langle (f_1)_{\mathrm{red}}\rangle + I$, where $(f_1)_{\mathrm{red}}$ is defined in §2.

§6 Decomposition of a Variety into Irreducibles

In the last section, we saw that irreducible varieties arise naturally in many contexts. It is natural to ask whether an arbitrary variety can be built up out of irreducibles. In this section, we explore this and related questions.

We begin by translating the *ascending chain condition* (ACC) for ideals (see §5 of Chapter 2) into the language of varieties.

Proposition 1 (The Descending Chain Condition). *Any descending chain of varieties*
$$V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots$$
in k^n must stabilize, meaning that there exists a positive integer N such that $V_N = V_{N+1} = \cdots$.

Proof. Passing to the corresponding ideals gives an ascending chain of ideals

$$\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \subseteq \mathbf{I}(V_3) \subseteq \cdots .$$

By the ascending chain condition for ideals (see Theorem 7 of Chapter 2, §5), there exists N such that $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \cdots$. Since $\mathbf{V}(\mathbf{I}(V)) = V$ for any variety V, we have $V_N = V_{N+1} = \cdots$. □

We can use Proposition 1 to prove the following basic result about the structure of affine varieties.

Theorem 2. *Let $V \subseteq k^n$ be an affine variety. Then V can be written as a finite union*

$$V = V_1 \cup \cdots \cup V_m,$$

where each V_i is an irreducible variety.

Proof. Assume that V is an affine variety which cannot be written as a finite union of irreducibles. Then V is not irreducible, so that $V = V_1 \cup V_1'$, where $V \neq V_1$ and $V \neq V_1'$. Further, one of V_1 and V_1' must not be a finite union of irreducibles, for otherwise V would be of the same form. Say V_1 is not a finite union of irreducibles. Repeating the argument just given, we can write $V_1 = V_2 \cup V_2'$, where $V_1 \neq V_2$, $V_1 \neq V_2'$, and V_2 is not a finite union of irreducibles. Continuing in this way gives us an infinite sequence of affine varieties

$$V \supseteq V_1 \supseteq V_2 \supseteq \cdots$$

with

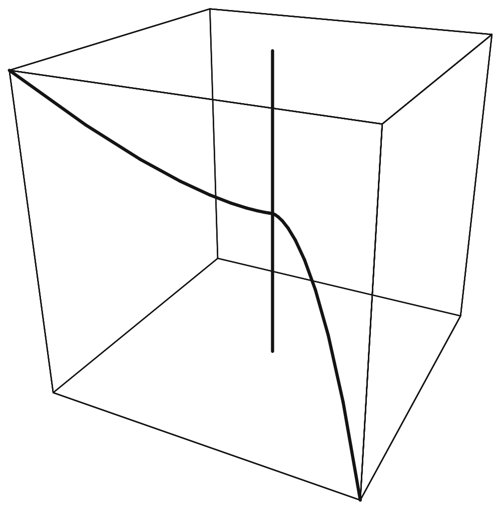
$$V \neq V_1 \neq V_2 \neq \cdots .$$

This contradicts Proposition 1. □

As a simple example of Theorem 2, consider the variety $\mathbf{V}(xz, yz)$ which is a union of a line (the z-axis) and a plane [the (x,y)-plane], both of which are irreducible by Exercise 6 of §5. For a more complicated example of the decomposition of a variety into irreducibles, consider the variety

$$V = \mathbf{V}(xz - y^2, x^3 - yz).$$

A sketch of this variety appears at the top of the next page. The picture suggests that this variety is not irreducible. It appears to be a union of two curves. Indeed, since both $xz - y^2$ and $x^3 - yz$ vanish on the z-axis, it is clear that the z-axis $\mathbf{V}(x,y)$ is contained in V. What about the other curve $V \setminus \mathbf{V}(x,y)$?



By Corollary 11 of §4, this suggests looking at the ideal quotient

$$\langle xz - y^2, x^3 - yz\rangle : \langle x, y\rangle.$$

(At the end of the section we will see that $\langle xz - y^2, x^3 - yz\rangle$ is a radical ideal.) We can compute this quotient using our algorithm for computing ideal quotients (make sure you review this algorithm). By equation (5) of §4, the above is equal to

$$(I : x) \cap (I : y),$$

where $I = \langle xz - y^2, x^3 - yz\rangle$. To compute $I : x$, we first compute $I \cap \langle x\rangle$ using our algorithm for computing intersections of ideals. Using lex order with $z > y > x$, we obtain

$$I \cap \langle x\rangle = \langle x^2z - xy^2, x^4 - xyz, x^3y - xz^2, x^5 - xy^3\rangle.$$

We can omit $x^5 - xy^3$ since it is a combination of the first and second elements in the basis. Hence

$$\begin{aligned} I : x &= \left\langle \frac{x^2z - xy^2}{x}, \frac{x^4 - xyz}{x}, \frac{x^3y - xz^2}{x} \right\rangle \\ &= \langle xz - y^2, x^3 - yz, x^2y - z^2\rangle \\ &= I + \langle x^2y - z^2\rangle. \end{aligned} \tag{1}$$

Similarly, to compute $I : \langle y\rangle$, we compute

$$I \cap \langle y\rangle = \langle xyz - y^3, x^3y - y^2z, x^2y^2 - yz^2\rangle,$$

which gives

$$\begin{aligned} I : y &= \left\langle \frac{xyz - y^3}{y}, \frac{x^3y - y^2z}{y}, \frac{x^2y^2 - yz^2}{y} \right\rangle \\ &= \langle xz\ - y^2, x^3 - yz, x^2y - z^2 \rangle \\ &= I + \langle x^2y - z^2 \rangle \\ &= I : x. \end{aligned}$$

(Do the computations using a computer algebra system.) Since $I : x = I : y$, we have

$$I : \langle x, y \rangle = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle.$$

The variety $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ turns out to be an irreducible curve. To see this, note that it can be parametrized as (t^3, t^4, t^5) [it is clear that $(t^3, t^4, t^5) \in W$ for any t—we leave it as an exercise to show every point of W is of this form], so that W is irreducible by Proposition 5 of the last section. It then follows easily that

$$V = \mathbf{V}(I) = \mathbf{V}(x, y) \cup \mathbf{V}(I : \langle x, y \rangle) = \mathbf{V}(x, y) \cup W$$

(see Proposition 7 of §4), which gives decomposition of V into irreducibles.

Both in the above example and the case of $\mathbf{V}(xz, yz)$, it appears that the decomposition of a variety into irreducible pieces is unique. It is natural to ask whether this is true in general. It is clear that, to avoid trivialities, we must rule out decompositions in which the same irreducible piece appears more than once, or in which one irreducible piece contains another. This is the aim of the following definition.

Definition 3. Let $V \subseteq k^n$ be an affine variety. A decomposition

$$V = V_1 \cup \cdots \cup V_m,$$

where each V_i is an irreducible variety, is called a **minimal decomposition** (or, sometimes, an **irredundant union**) if $V_i \not\subseteq V_j$ for $i \neq j$. Also, we call the V_i the **irreducible components** of V.

With this definition, we can now prove the following uniqueness result.

Theorem 4. *Let $V \subseteq k^n$ be an affine variety. Then V has a minimal decomposition*

$$V = V_1 \cup \cdots \cup V_m$$

(so each V_i is an irreducible variety and $V_i \not\subseteq V_j$ for $i \neq j$). Furthermore, this minimal decomposition is unique up to the order in which $V_1, \ldots, V_m$ are written.

Proof. By Theorem 2, V can be written in the form $V = V_1 \cup \cdots \cup V_m$, where each V_i is irreducible. Further, if a V_i lies in some V_j for $i \neq j$, we can drop V_i, and V will be the union of the remaining V_j's for $j \neq i$. Repeating this process leads to a minimal decomposition of V.

To show uniqueness, suppose that $V = V_1' \cup \cdots \cup V_l'$ is another minimal decomposition of V. Then, for each V_i in the first decomposition, we have

$$V_i = V_i \cap V = V_i \cap (V_1' \cup \cdots \cup V_l') = (V_i \cap V_1') \cup \cdots \cup (V_i \cap V_l').$$

Since V_i is irreducible, it follows that $V_i = V_i \cap V_j'$ for some j, i.e., $V_i \subseteq V_j'$. Applying the same argument to V_j' (using the V_i's to decompose V) shows that $V_j' \subseteq V_k$ for some k, and, thus,

$$V_i \subseteq V_j' \subseteq V_k.$$

By minimality, $i = k$, and it follows that $V_i = V_j'$. Hence, every V_i appears in $V = V_1' \cup \cdots \cup V_l'$, which implies $m \leq l$. A similar argument proves $l \leq m$, and $m = l$ follows. Thus, the V_i''s are just a permutation of the V_i's, and uniqueness is proved. □

The uniqueness part of Theorem 4 guarantees that the irreducible components of V are well-defined. We remark that the uniqueness is false if one does not insist that the union be finite. (A plane P is the union of all the points on it. It is also the union of some line in P and all the points not on the line—there are infinitely many lines in P with which one could start.) This should alert the reader to the fact that although the proof of Theorem 4 is easy, it is far from vacuous: one makes subtle use of finiteness (which follows, in turn, from the Hilbert Basis Theorem).

Here is a result that relates irreducible components to Zariski closure.

Proposition 5. *Let V, W be varieties with $W \subsetneq V$. Then $V \setminus W$ is Zariski dense in V if and only if W contains no irreducible component of V.*

Proof. Suppose that $V = V_1 \cup \cdots \cup V_m$ as in Theorem 4 and that $V_i \not\subseteq W$ for all i. This implies $V_i \cap W \subsetneq V_i$, and since V_i is irreducible, we deduce $\overline{V_i \setminus (V_i \cap W)} = V_i$ by Proposition 13 of §5. Then

$$\begin{aligned}\overline{V \setminus W} = \overline{(V_1 \cup \cdots \cup V_m) \setminus W} &= \overline{(V_1 \setminus (V_1 \cap W)) \cup \cdots \cup (V_m \setminus (V_m \cap W))} \\ &= \overline{V_1 \setminus (V_1 \cap W)} \cup \cdots \cup \overline{V_m \setminus (V_m \cap W)} \\ &= V_1 \cup \cdots \cup V_m = V,\end{aligned}$$

where the second line uses Lemma 3 of §4. The other direction of the proof will be covered in the exercises. □

Theorems 2 and 4 can also be expressed purely algebraically using the one-to-one correspondence between radical ideals and varieties.

Theorem 6. *If k is algebraically closed, then every radical ideal in $k[x_1, \ldots, x_n]$ can be written uniquely as a finite intersection of prime ideals $P_1 \cap \cdots \cap P_r$, where $P_i \not\subseteq P_j$ for $i \neq j$. (As in the case of varieties, we often call such a presentation of a radical ideal a* **minimal decomposition** *or an* **irredundant intersection***).*

Proof. Theorem 6 follows immediately from Theorems 2 and 4 and the ideal–variety correspondence. □

We can also use ideal quotients from §4 to describe the prime ideals that appear in the minimal representation of a radical ideal.

Theorem 7. *If k is algebraically closed and I is a proper radical ideal such that*

$$I = \bigcap_{i=1}^{r} P_i$$

is its minimal decomposition as an intersection of prime ideals, then the P_i's are precisely the proper prime ideals that occur in the set $\{I : f \mid f \in k[x_1, \ldots, x_n]\}$.

Proof. First, note that since I is proper, each P_i is also a proper ideal (this follows from minimality).

For any $f \in k[x_1, \ldots, x_n]$, we have

$$I : f = \Big(\bigcap_{i=1}^{r} P_i\Big) : f = \bigcap_{i=1}^{r} (P_i : f)$$

by Exercise 17 of §4. Note also that for any prime ideal P, either $f \in P$, in which case $P : f = \langle 1 \rangle$, or $f \notin P$, in which case $P : f = P$ (see Exercise 3).

Now suppose that $I : f$ is a proper prime ideal. By Exercise 4 of §5, the above formula for $I : f$ implies that $I : f = P_i : f$ for some i. Since $P_i : f = P_i$ or $\langle 1 \rangle$ by the above observation, it follows that $I : f = P_i$.

To see that every P_i can arise in this way, fix i and pick $f \in \big(\bigcap_{j \neq i}^{r} P_j\big) \setminus P_i$; such an f exists because $\bigcap_{i=1}^{r} P_i$ is minimal. Then $P_i : f = P_i$ and $P_j : f = \langle 1 \rangle$ for $j \neq i$. If we combine this with the above formula for $I : f$, then it follows that $I : f = P_i$. □

We should mention that Theorems 6 and 7 hold for any field k, although the proofs in the general case are different (see Corollary 10 of §8).

For an example of these theorems, consider the ideal $I = \langle xz - y^2, x^3 - yz \rangle$. Recall that the variety $V = \mathbf{V}(I)$ was discussed earlier in this section. For the time being, let us assume that I is radical (eventually we will see that this is true). Can we write I as an intersection of prime ideals?

We start with the geometric decomposition

$$V = \mathbf{V}(x, y) \cup W$$

proved earlier, where $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$. This suggests that

$$I = \langle x, y \rangle \cap \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle,$$

which is straightforward to prove by the techniques we have learned so far (see Exercise 4). Also, from equation (1), we know that $I : x = \langle xz - y^2, x^3 - yz, x^2y - z^2 \rangle$. Thus,

$$I = \langle x, y \rangle \cap (I : x).$$

To represent $\langle x, y\rangle$ as an ideal quotient of I, let us think geometrically. The idea is to remove W from V. Of the three equations defining W, the first two give V. So it makes sense to use the third one, $x^2y - z^2$, and one can check that $I:(x^2y - z^2) = \langle x, y\rangle$ (see Exercise 4). Thus,

$$I = (I:(x^2y - z^2)) \cap (I:x). \tag{2}$$

It remains to show that $I:(x^2y - z^2)$ and $I:x$ are prime ideals. The first is easy since $I:(x^2y - z^2) = \langle x, y\rangle$ is obviously prime. As for the second, we have already seen that $W = \mathbf{V}(xz - y^2, x^3 - yz, x^2y - z^2)$ is irreducible and, in the exercises, you will show that $\mathbf{I}(W) = \langle xz - y^2, x^3 - yz, x^2y - z^2\rangle = I:x$. It follows from Proposition 3 of §5 that $I:x$ is a prime ideal. This completes the proof that (2) is the minimal representation of I as an intersection of prime ideals. Finally, since I is an intersection of prime ideals, we see that I is a radical ideal (see Exercise 1).

The arguments used in this example are special to the case $I = \langle xz - y^2, x^3 - yz\rangle$. It would be nice to have more general methods that could be applied to any ideal. Theorems 2, 4, 6, and 7 tell us that certain decompositions exist, but the proofs give no indication of how to find them. The problem is that the proofs rely on the Hilbert Basis Theorem, which is intrinsically nonconstructive. Based on what we have seen in §§5 and 6, the following questions arise naturally:

- (Primality) Is there an algorithm for deciding if a given ideal is prime?
- (Irreducibility) Is there an algorithm for deciding if a given affine variety is irreducible?
- (Decomposition) Is there an algorithm for finding the minimal decomposition of a given variety or radical ideal?

The answer to all three questions is *yes*, and descriptions of the algorithms can be found in the works of HERMANN (1926), MINES, RICHMAN, and RUITENBERG (1988), and SEIDENBERG (1974, 1984). As in §2, the algorithms in these articles are very inefficient. However, the work of GIANNI, TRAGER and ZACHARIAS (1988) and EISENBUD, HUNEKE and VASCONCELOS (1992) has led to more efficient algorithms. See also Chapter 8 of BECKER and WEISPFENNING (1993) and §4.4 of ADAMS and LOUSTAUNAU (1994).

EXERCISES FOR §6

1. Show that the intersection of any collection of prime ideals is radical.
2. Show that an irredundant intersection of at least two prime ideals is never prime.
3. If $P \subseteq k[x_1, \ldots, x_n]$ is a prime ideal, then prove that $P:f = P$ if $f \notin P$ and $P:f = \langle 1\rangle$ if $f \in P$.
4. Let $I = \langle xz - y^2, x^3 - yz\rangle$.
   a. Show that $I:(x^2y - z^2) = \langle x, y\rangle$.
   b. Show that $I:(x^2y - z^2)$ is prime.
   c. Show that $I = \langle x, y\rangle \cap \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle$.
5. Let $J = \langle xz - y^2, x^3 - yz, z^2 - x^2y\rangle \subseteq k[x, y, z]$, where k is infinite.
   a. Show that every point of $W = \mathbf{V}(J)$ is of the form (t^3, t^4, t^5) for some $t \in k$.

b. Show that $J = \mathbf{I}(W)$. Hint: Compute a Gröbner basis for J using lex order with $z > y > x$ and show that every $f \in k[x, y, z]$ can be written in the form

$$f = g + a + bz + xA(x) + yB(x) + y^2C(x),$$

where $g \in J, a, b \in k$ and $A, B, C \in k[x]$.

6. Complete the proof of Proposition 5. Hint: $V_i \subseteq W$ implies $V \setminus W \subseteq V \setminus V_i$.
7. Translate Theorem 7 and its proof into geometry.
8. Let $I = \langle xz - y^2, z^3 - x^5\rangle \subseteq \mathbb{Q}[x, y, z]$.
   a. Express $\mathbf{V}(I)$ as a finite union of irreducible varieties. Hint: The parametrizations (t^3, t^4, t^5) and $(t^3, -t^4, t^5)$ will be useful.
   b. Express I as an intersection of prime ideals which are ideal quotients of I and conclude that I is radical.
9. Let V, W be varieties in k^n with $V \subseteq W$. Show that each irreducible component of V is contained in some irreducible component of W.
10. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ and let $f = f_1^{a_1} f_2^{a_2} \cdots f_r^{a_r}$ be the decomposition of f into irreducible factors. Show that $\mathbf{V}(f) = \mathbf{V}(f_1) \cup \cdots \cup \mathbf{V}(f_r)$ is the decomposition of $\mathbf{V}(f)$ into irreducible components and $\mathbf{I}(\mathbf{V}(f)) = \langle f_1 f_2 \cdots f_r\rangle$. Hint: See Exercise 11 of §5.

§7 Proof of the Closure Theorem

This section will complete the proof of the Closure Theorem from Chapter 3, §2. We will use many of the tools introduced in this chapter, including the Nullstellensatz, Zariski closures, saturations, and irreducible components.

We begin by recalling the basic situation. Let k be an algebraically closed field, and let $\pi_l : k^n \to k^{n-l}$ is projection onto the last $n - l$ components. If $V = \mathbf{V}(I)$ is an affine variety in k^n, then we get the l-th elimination ideal $I_l = I \cap k[x_{l+1}, \ldots, x_n]$. The first part of the Closure Theorem, which asserts that $\mathbf{V}(I_l)$ is the Zariski closure of $\pi_l(V)$ in k^{n-l}, was proved earlier in Theorem 4 of §4.

The remaining part of the Closure Theorem tells us that $\pi_l(V)$ fills up "most" of $\mathbf{V}(I_l)$. Here is the precise statement.

Theorem 1 (The Closure Theorem, second part). *Let k be algebraically closed, and let $V = \mathbf{V}(I) \subseteq k^n$. Then there is an affine variety $W \subseteq \mathbf{V}(I_l)$ such that*

$$\mathbf{V}(I_l) \setminus W \subseteq \pi_l(V) \text{ and } \overline{\mathbf{V}(I_l) \setminus W} = \mathbf{V}(I_l).$$

This is slightly different from the Closure Theorem stated in §2 of Chapter 3. There, we assumed $V \neq \emptyset$ and asserted that $\mathbf{V}(I_l) \setminus W \subseteq \pi_l(V)$ for some $W \subsetneq \mathbf{V}(I_l)$. In Exercise 1 you will prove that Theorem 1 implies the version in Chapter 3.

The proof of Theorem 1 will use the following notation. Rename $x_{l+1}, \ldots, x_n$ as $y_{l+1}, \ldots, y_n$ and write $k[x_1, \ldots, x_l, y_{l+1}, \ldots, y_n]$ as $k[\mathbf{x}, \mathbf{y}]$ for $\mathbf{x} = (x_1, \ldots, x_l)$ and $\mathbf{y} = (y_{l+1}, \ldots, y_n)$. Also fix a monomial order $>$ on $k[\mathbf{x}, \mathbf{y}]$ with the property that $\mathbf{x}^\alpha > \mathbf{x}^\beta$ implies $\mathbf{x}^\alpha > \mathbf{x}^\beta \mathbf{y}^\gamma$ for all γ. The product order described in Exercise 9 of Chapter 2, §4 is an example of such a monomial order. Another example is given by lex order with $x_1 > \cdots > x_l > y_{l+1} > \cdots > y_n$.

An important tool in proving Theorem 1 is the following result.

Theorem 2. *Fix a field k. Let $I \subseteq k[\mathbf{x},\mathbf{y}]$ be an ideal and let $G = \{g_1,\ldots,g_t\}$ be a Gröbner basis for I with respect to a monomial order as above. For $1 \le i \le t$ with $g_i \notin k[\mathbf{y}]$, write g_i in the form*

$$(1) \qquad g_i = c_i(\mathbf{y})\,\mathbf{x}^{\alpha_i} + \textit{terms} < \mathbf{x}^{\alpha_i}.$$

Finally, assume that $\mathbf{b} = (a_{l+1},\ldots,a_n) \in \mathbf{V}(I_l) \subseteq k^{n-l}$ is a partial solution such that $c_i(\mathbf{b}) \neq 0$ for all $g_i \notin k[\mathbf{y}]$. Then:

(i) *The set*
$$\overline{G} = \{g_i(\mathbf{x},\mathbf{b}) \mid g_i \notin k[\mathbf{y}]\} \subseteq k[\mathbf{x}]$$
is a Gröbner basis of the ideal $\{f(\mathbf{x},\mathbf{b}) \mid f \in I\}$.

(ii) *If k is algebraically closed, then there exists $\mathbf{a} = (a_1,\ldots,a_l) \in k^l$ such that $(\mathbf{a},\mathbf{b}) \in V = \mathbf{V}(I)$.*

Proof. Given $f \in k[\mathbf{x},\mathbf{y}]$, we set

$$\bar{f} = f(\mathbf{x},\mathbf{b}) \in k[\mathbf{x}].$$

In this notation, $\overline{G} = \{\bar{g}_i \mid g_i \notin k[\mathbf{y}]\}$. Also observe that $\bar{g}_i = 0$ when $g_i \in k[\mathbf{y}]$ since $\mathbf{b} \in \mathbf{V}(I_l)$. If we set $\bar{I} = \{\bar{f} \mid f \in I\}$, then it is an easy exercise to show that

$$\bar{I} = \langle \overline{G} \rangle \subseteq k[\mathbf{x}].$$

In particular, $\bar{I}$ is an ideal of $k[\mathbf{x}]$.

To prove that $\overline{G}$ is a Gröbner basis of $\bar{I}$, take $g_i, g_j \in G \setminus k[\mathbf{y}]$ and consider the polynomial

$$S = c_j(\mathbf{y})\,\frac{\mathbf{x}^{\gamma}}{\mathbf{x}^{\alpha_i}}\,g_i - c_i(\mathbf{y})\,\frac{\mathbf{x}^{\gamma}}{\mathbf{x}^{\alpha_j}}\,g_j,$$

where $\mathbf{x}^{\gamma} = \operatorname{lcm}(\mathbf{x}^{\alpha_i},\mathbf{x}^{\alpha_j})$. Our chosen monomial order has the property that $\mathrm{LT}(g_i) = \mathrm{LT}(c_i(\mathbf{y}))\mathbf{x}^{\alpha_i}$, and it follows easily that $\mathbf{x}^{\gamma} > \mathrm{LT}(S)$. Since $S \in I$, it has a standard representation $S = \sum_{k=1}^{t} A_k g_k$. Then evaluating at $\mathbf{b}$ gives

$$c_j(\mathbf{b})\,\frac{\mathbf{x}^{\gamma}}{\mathbf{x}^{\alpha_i}}\,\bar{g}_i - c_i(\mathbf{b})\,\frac{\mathbf{x}^{\gamma}}{\mathbf{x}^{\alpha_j}}\,\bar{g}_j = \overline{S} = \textstyle\sum_{\bar{g}_k \in \overline{G}} \overline{A}_k \bar{g}_k$$

since $\bar{g}_i = 0$ for $g_i \in k[\mathbf{y}]$.

Then $c_i(\mathbf{b}), c_j(\mathbf{b}) \neq 0$ imply that $\overline{S}$ is the S-polynomial $S(\bar{g}_i,\bar{g}_j)$ up to the nonzero constant $c_i(\mathbf{b})c_j(\mathbf{b})$. Since

$$\mathbf{x}^{\gamma} > \mathrm{LT}(S) \ge \mathrm{LT}(A_k g_k), \quad A_k g_k \neq 0,$$

it follows that

$$\mathbf{x}^{\gamma} > \mathrm{LT}(\bar{A}_k \bar{g}_k), \quad \bar{A}_k \bar{g}_k \neq 0,$$

by Exercise 3 of Chapter 2, §9. Hence $S(\bar{g}_i, \bar{g}_j)$ has an lcm representation as defined in Chapter 2, §9. By Theorem 6 of that section, we conclude that $\overline{G}$ is a Gröbner basis of $\bar{I}$, as claimed.

For part (ii), note that by construction, every element of $\overline{G}$ has positive total degree in the $\mathbf{x}$ variables, so that $\bar{g}_i$ is nonconstant for every i. It follows that $1 \notin \bar{I}$ since $\overline{G}$ is a Gröbner basis of $\bar{I}$. Hence $\bar{I} \subsetneq k[\mathbf{x}]$, so that by the Nullstellensatz, there exists $\mathbf{a} \in k^l$ such that $\bar{g}_i(\mathbf{a}) = 0$ for all $\bar{g}_i \in \overline{G}$, i.e., $g_i(\mathbf{a}, \mathbf{b}) = 0$ for all $g_i \in G \setminus k[\mathbf{y}]$. Since $\bar{g}_i = 0$ when $g_i \in k[\mathbf{y}]$, it follows that $g_i(\mathbf{a}, \mathbf{b}) = 0$ for all $g_i \in G$. Hence $(\mathbf{a}, \mathbf{b}) \in V = \mathbf{V}(I)$. □

Part (ii) of Theorem 2 is related to the Extension Theorem from Chapter 3. Compared to the Extension theorem, part (ii) is simultaneously stronger (the Extension Theorem assumes $l = 1$, i.e., just one variable is eliminated) and weaker [part (ii) requires the nonvanishing of *all* relevant leading coefficients, while the Extension Theorem requires just one].

For our purposes, Theorem 2 has the following important corollary.

Corollary 3. *With the same notation as Theorem 2, we have*

$$\mathbf{V}(I_l) \setminus \mathbf{V}\big(\textstyle\prod_{g_i \in G\setminus k[\mathbf{y}]} c_i\big) \subseteq \pi_l(V).$$

Proof. Take $\mathbf{b} \in \mathbf{V}(I_l) \setminus \mathbf{V}\big(\prod_{g_i \in G\setminus k[\mathbf{y}]} c_i\big)$. Then $\mathbf{b} \in \mathbf{V}(I_l)$ and $c_i(\mathbf{b}) \neq 0$ for all $g_i \in G \setminus k[\mathbf{y}]$. By Theorem 2, there is $\mathbf{a} \in k^l$ such that $(\mathbf{a}, \mathbf{b}) \in V = \mathbf{V}(I)$. In other words, $\mathbf{b} \in \pi_l(V)$, and the corollary follows. □

Since $A \setminus B = A \setminus (A \cap B)$, Corollary 3 implies that the intersection

$$W = \mathbf{V}(I_l) \cap \mathbf{V}\big(\textstyle\prod_{g_i \in G\setminus k[\mathbf{y}]} c_i\big) \subseteq \mathbf{V}(I_l)$$

has the property that $\mathbf{V}(I_l) \setminus W \subseteq \pi_l(V)$. If $\mathbf{V}(I_l) \setminus W$ is also Zariski dense in $\mathbf{V}(I_l)$, then $W \subseteq \mathbf{V}(I_l)$ satisfies the conclusion of the Closure Theorem.

Hence, to complete the proof of the Closure Theorem, we need to explore what happens when the difference $\mathbf{V}(I_l) \setminus \mathbf{V}\big(\prod_{g_i \in G\setminus k[\mathbf{y}]} c_i\big)$ is not Zariski dense in $\mathbf{V}(I_l)$. The following proposition shows that in this case, the original variety $V = \mathbf{V}(I)$ decomposes into varieties coming from strictly bigger ideals.

Proposition 4. *Assume that k is algebraically closed and the Gröbner basis G is reduced. If $\mathbf{V}(I_l) \setminus \mathbf{V}\big(\prod_{g_i \in G\setminus k[\mathbf{y}]} c_i\big)$ is not Zariski dense in $\mathbf{V}(I_l)$, then there is some $g_i \in G \setminus k[\mathbf{y}]$ whose c_i has the following two properties:*

(i) $V = \mathbf{V}(I + \langle c_i \rangle) \cup \mathbf{V}(I : c_i^\infty)$.

(ii) $I \subsetneq I + \langle c_i \rangle$ *and* $I \subsetneq I : c_i^\infty$.

Proof. For (i), we have $V = \mathbf{V}(I) = \mathbf{V}(I + \langle c_i \rangle) \cup \mathbf{V}(I : c_i^\infty)$ by Theorem 10 of §4.

For (ii), we first show that $I \subsetneq I + \langle c_i \rangle$ for all $g_i \in G \setminus k[\mathbf{y}]$. To see why, suppose that $c_i \in I$ for some i. Since G is a Gröbner basis of I, $\mathrm{LT}(c_i)$ is divisible by some $\mathrm{LT}(g_j)$, and then $g_j \in k[\mathbf{y}]$ since the monomial order eliminates the $\mathbf{x}$ variables.

Hence $g_j \neq g_i$. But then (1) implies that $\text{LT}(g_j)$ divides $\text{LT}(g_i) = \text{LT}(c_i)\mathbf{x}^{\alpha_i}$, which contradicts our assumption that G is reduced. Hence $c_i \notin I$, and $I \subsetneq I + \langle c_i \rangle$ follows.

Now suppose that $I = I : c_i^\infty$ for all i with $g_i \in G \setminus k[\mathbf{y}]$. In Exercise 4, you will show that this implies $I_l : c_i^\infty = I_l$ for all i. Hence

$$\mathbf{V}(I_l) = \mathbf{V}(I_l : c_i^\infty) = \overline{\mathbf{V}(I_l) \setminus \mathbf{V}(c_i)} = \overline{\mathbf{V}(I_l) \setminus (\mathbf{V}(I_l) \cap \mathbf{V}(c_i))},$$

where the second equality uses Theorem 10 of §4. If follows that $\mathbf{V}(I_l) \cap \mathbf{V}(c_i)$ contains no irreducible component of $\mathbf{V}(I_l)$ by Proposition 5 of §6. Since this holds for all i, the finite union

$$\textstyle\bigcup_{g_i \in G \setminus k[\mathbf{y}]} \mathbf{V}(I_l) \cap \mathbf{V}(c_i) = \mathbf{V}(I_l) \cap \bigcup_{g_i \in G \setminus k[\mathbf{y}]} \mathbf{V}(c_i) = \mathbf{V}(I_l) \cap \mathbf{V}\big(\prod_{g_i \in G \setminus k[\mathbf{y}]} c_i\big)$$

also contains no irreducible component of $\mathbf{V}(I_l)$ (see Exercise 5). By the same proposition from §6, we conclude that the difference

$$\mathbf{V}(I_l) \setminus \big(\mathbf{V}(I_l) \cap \mathbf{V}\big(\textstyle\prod_{g_i \in G \setminus k[\mathbf{y}]} c_i\big)\big) = \mathbf{V}(I_l) \setminus \mathbf{V}\big(\prod_{g_i \in G \setminus k[\mathbf{y}]} c_i\big)$$

is Zariski dense in $\mathbf{V}(I_l)$. This contradiction shows that $I \subsetneq I : c_i^\infty$ for some i and completes the proof of the proposition. $\square$

In the situation of Proposition 4, we have a decomposition of V into two pieces. The next step is to show that if we can find a W that works for each piece, then we can find a W what works for V. Here is the precise result.

Proposition 5. *Let k be algebraically closed. Suppose that a variety $V = \mathbf{V}(I)$ can be written $V = \mathbf{V}(I^{(1)}) \cup \mathbf{V}(I^{(2)})$ and that we have varieties*

$$W_1 \subseteq \mathbf{V}(I_l^{(1)}) \quad \textit{and} \quad W_2 \subseteq \mathbf{V}(I_l^{(2)})$$

such that $\overline{\mathbf{V}(I_l^{(i)}) \setminus W_i} = \mathbf{V}(I_l^{(i)})$ and $\mathbf{V}(I_l^{(i)}) \setminus W_i \subseteq \pi_l(\mathbf{V}(I^{(i)})$ for $i = 1, 2$. Then $W = W_1 \cup W_2$ is a variety contained in V that satisfies

$$\overline{\mathbf{V}(I_l) \setminus W} = \mathbf{V}(I_l) \quad \textit{and} \quad \mathbf{V}(I_l) \setminus W \subseteq \pi_l(V).$$

Proof. For simplicity, set $V_i = \mathbf{V}(I^{(i)})$, so that $V = V_1 \cup V_2$. The first part of the Closure Theorem proved in §4 implies that $\mathbf{V}(I_l) = \overline{\pi_l(V)}$ and $\mathbf{V}(I_l^{(i)}) = \overline{\pi_l(V_i)}$. Hence

$$\begin{aligned} \mathbf{V}(I_l) = \overline{\pi_l(V)} = \overline{\pi_l(V_1 \cup V_2)} = \overline{\pi_l(V_1) \cup \pi_l(V_2)} &= \overline{\pi_l(V_1)} \cup \overline{\pi_l(V_2)} \\ &= \mathbf{V}(I_l^{(1)}) \cup \mathbf{V}(I_l^{(2)}), \end{aligned}$$

where the last equality of the first line uses Lemma 3 of §4.

Now let $W_i \subseteq \mathbf{V}(I_l^{(i)})$ be as in the statement of the proposition. By Proposition 5 of §6, we know that W_i contains no irreducible component of $\mathbf{V}(I_l^{(i)})$. As you will prove in Exercise 5, this implies that the union $W = W_1 \cup W_2$ contains no irreducible component of $\mathbf{V}(I_l) = \mathbf{V}(I_l^{(1)}) \cup \mathbf{V}(I_l^{(2)})$. Using Proposition 5 of §6 again, we deduce that $\mathbf{V}(I_l) \setminus W$ is Zariski dense in $\mathbf{V}(I_l)$. Since we also have

$$\begin{aligned}\mathbf{V}(I_l) \setminus W = \big(\mathbf{V}(I_l^{(1)}) \cup \mathbf{V}(I_l^{(2)})\big) \setminus (W_1 \cup W_2) &\subseteq \big(\mathbf{V}(I_l^{(1)}) \setminus W_1\big) \cup \big(\mathbf{V}(I_l^{(2)}) \setminus W_2\big)\\ &\subseteq \pi_l(V_1) \cup \pi_l(V_2) = \pi_l(V),\end{aligned}$$

the proof of the proposition is complete. □

The final ingredient we need for the proof of the Closure Theorem is the following maximum principle for ideals.

Proposition 6 (Maximum Principle for Ideals). *Given a nonempty collection of ideals $\{I_\alpha\}_{\alpha \in \mathcal{A}}$ in a polynomial ring $k[x_1, \dots, x_n]$, there exists $\alpha_0 \in \mathcal{A}$ such that for all $\beta \in \mathcal{A}$, we have*

$$I_{\alpha_0} \subseteq I_\beta \Longrightarrow I_{\alpha_0} = I_\beta.$$

In other words, I_{α_0} is maximal with respect to inclusion among the I_α for $\alpha \in \mathcal{A}$.

Proof. This is an easy consequence of the ascending chain condition (Theorem 7 of Chapter 2, §5). The proof will be left as an exercise. □

We are now ready to prove the second part of the Closure Theorem.

Proof of Theorem 1. Suppose the theorem fails for some ideal $I \subseteq k[x_1, \dots, x_n]$, i.e., there is no affine variety $W \subsetneq \mathbf{V}(I)$ such that

$$\mathbf{V}(I_l) \setminus W \subseteq \pi_l(\mathbf{V}(I)) \text{ and } \overline{\mathbf{V}(I_l) \setminus W} = \mathbf{V}(I_l).$$

Our goal is to derive a contradiction.

Among all ideals for which the theorem fails, the maximum principle of Proposition 6 guarantees that there is a maximal such ideal, i.e., there is an ideal I such that the theorem fails for I but holds for every strictly larger ideal $I \subsetneq J$.

Let us apply our results to I. By Corollary 3, we know that

$$\mathbf{V}(I_l) \setminus \mathbf{V}\big(\textstyle\prod_{g_i \in G \setminus k[\mathbf{y}]} c_i\big) \subseteq \pi_l(V).$$

Since the theorem fails for I, $\mathbf{V}(I) \setminus \mathbf{V}\big(\prod_{g_i \in G \setminus k[\mathbf{y}]} c_i\big)$ cannot be Zariski dense in $\mathbf{V}(I_l)$. Therefore, by Proposition 4, there is some i such that

$$I \subsetneq I^{(1)} = I + \langle c_i \rangle, \quad I \subsetneq I^{(2)} = I : c_i^\infty$$

and

$$\mathbf{V}(I) = \mathbf{V}(I^{(1)}) \cup \mathbf{V}(I^{(2)}).$$

Our choice of I guarantees that the theorem holds for the strictly larger ideals $I^{(1)}$ and $I^{(2)}$. The resulting affine varieties $W_i \subseteq \mathbf{V}(I_l^{(i)})$, $i = 1, 2$, satisfy the hypothesis of Proposition 5, and then the proposition implies that $W = W_1 \cup W_2 \subseteq \mathbf{V}(I)$ satisfies the theorem for I. This contradicts our choice of I, and we are done. □

The proof of the Closure Theorem just given is nonconstructive. Fortunately, in practice it is straightforward to find $W \subseteq \mathbf{V}(I_l)$ with the required properties. We will give two examples and then describe a general procedure.

The first example is very simple. Consider the ideal

$$I = \langle yx^2 + yx + 1 \rangle \subseteq \mathbb{C}[x, y].$$

We use lex order with $x > y$, and $I_1 = \{0\}$ since $g_1 = yx^2 + yx + 1$ is a Gröbner basis for I. In the notation of Theorem 2, we have $c_1 = y$, and then Corollary 3 implies that

$$\mathbf{V}(I_1) \setminus \mathbf{V}(c_1) = \mathbb{C} \setminus \mathbf{V}(y) = \mathbb{C} \setminus \{0\} \subseteq \pi_1(\mathbf{V}(I)) = \mathbb{C}.$$

Hence, we can take $W = \{0\}$ in Theorem 1 since $\mathbb{C} \setminus \{0\}$ is Zariski dense in $\mathbb{C}$.

The second example, taken from SCHAUENBURG (2007), uses the ideal

$$I = \langle xz + y - 1, w + y + z - 2, z^2 \rangle \subseteq \mathbb{C}[w, x, y, z].$$

It is straightforward to check that $V = \mathbf{V}(I)$ is the line $V = \mathbf{V}(w-1, y-1, z) \subseteq \mathbb{C}^4$, which projects to the point $\pi_2(V) = \mathbf{V}(y - 1, z) \subseteq \mathbb{C}^2$ when we eliminate w and x. Thus, $W = \emptyset$ satisfies Theorem 1 in this case.

Here is a systematic way to discover that $W = \emptyset$. A lex Gröbner basis of I for $w > x > y > z$ consists of

$$g_1 = w + y + z - 2,\ g_2 = xz + y - 1,\ g_3 = y^2 - 2y + 1,\ g_4 = yz - z,\ g_5 = z^2.$$

Eliminating w and x gives $I_2 = \langle g_3, g_4, g_5 \rangle$, and one sees easily that

$$\mathbf{V}(I_2) = \mathbf{V}(y - 1, z).$$

Since $g_1 = 1 \cdot w + y + z - 2$ and $g_2 = z \cdot x + y - 1$, we have $c_1 = 1$ and $c_2 = z$. If we set

$$J = \langle c_1 c_2 \rangle = \langle z \rangle,$$

then Corollary 3 implies that $\mathbf{V}(I_2) \setminus \mathbf{V}(J) \subseteq \pi_2(V)$. However, $\mathbf{V}(I_2) \setminus \mathbf{V}(J) = \emptyset$, so the difference is not Zariski dense in $\mathbf{V}(I_2)$.

In this situation, we use the decomposition of $\mathbf{V}(I)$ guaranteed to exist by Proposition 4. Note that $I = I : c_1^\infty$ since $c_1 = 1$. Hence we use $c_2 = z$ in the proposition. This gives the two ideals

$$\begin{aligned} I^{(1)} &= I + \langle c_2 \rangle = \langle xz + y - 1, w + y + z - 2, z^2, z \rangle = \langle w - 1, y - 1, z \rangle, \\ I^{(2)} &= I : c_2^\infty = I : z^\infty = \langle 1 \rangle \text{ since } z^2 \in I. \end{aligned}$$

Now we start over with $I^{(1)}$ and $I^{(2)}$.

For $I^{(1)}$, observe that $\{w-1, y-1, z\}$ is a Gröbner basis of $I^{(1)}$, and only $g_1^{(1)} = w-1 \notin \mathbb{C}[y,z]$. The coefficient of w is $c_1^{(1)} = 1$, and then Corollary 3 applied to $I^{(1)}$ gives

$$\mathbf{V}(I_2^{(1)}) \setminus \mathbf{V}(1) \subseteq \pi_2(\mathbf{V}(I^{(1)})).$$

Since $\mathbf{V}(1) = \emptyset$, we can pick $W_1 = \emptyset$ for $I^{(1)}$ in Theorem 1.

Applying the same systematic process to $I^{(2)} = \langle 1 \rangle$, we see that there are *no* $g_i \notin \mathbb{C}[y,z]$. Thus Corollary 3 involves the product over the empty set. By convention (see Exercise 7) the empty product is 1. Then Corollary 3 tells us that we can pick $W_2 = \emptyset$ for $I^{(2)}$ in Theorem 1. By Proposition 5, it follows that Theorem 1 holds for the ideal I with

$$W = W_1 \cup W_2 = \emptyset \cup \emptyset = \emptyset.$$

To do this in general, we use the following recursive algorithm to produce the desired subset W:

Input : an ideal $I \subseteq k[\mathbf{x}, \mathbf{y}]$ with variety $V = \mathbf{V}(I)$

Output : $\text{FindW}(I) = W \subseteq \mathbf{V}(I_l)$ with $\mathbf{V}(I_l) \setminus W \subseteq \pi_l(V)$, $\overline{\mathbf{V}(I_l) \setminus W} = \mathbf{V}(I_l)$

$G :=$ reduced Gröbner basis for I for a monomial order as in Theorem 2

$c_i :=$ coefficient in $g_i = c_i(\mathbf{y})\mathbf{x}^{\alpha_i} + \text{terms} < \mathbf{x}^{\alpha_i}$ when $g_i \in G \setminus k[\mathbf{y}]$

$I_l := I \cap k[\mathbf{y}] = \langle G \cap k[\mathbf{y}] \rangle$

$J := \left\langle \prod_{g_i \in G \setminus k[\mathbf{y}]} c_i \right\rangle$

IF $\overline{\mathbf{V}(I_l) \setminus \mathbf{V}(J)} = \mathbf{V}(I_l)$ THEN

    $\text{FindW}(I) := \mathbf{V}(I_l) \cap \mathbf{V}(J)$

ELSE

    Select $g_i \in G \setminus k[\mathbf{y}]$ with $I \subsetneq I : c_i^\infty$

    $\text{FindW}(I) := \text{FindW}(I + \langle c_i \rangle) \cup \text{FindW}(I : c_i^\infty)$

RETURN FindW(I)

The function FindW takes the input ideal I and computes the ideals I_l and $J = \left\langle \prod_{g_i \in G \setminus k[\mathbf{y}]} c_i \right\rangle$. The IF statement asks whether $\mathbf{V}(I_l) \setminus \mathbf{V}(J)$ is Zariski dense in $\mathbf{V}(I_l)$. If the answer is yes, then $\mathbf{V}(I_l) \cap \mathbf{V}(J)$ has the desired property by Corollary 3, which is why $\text{FindW}(I) = \mathbf{V}(I_l) \cap \mathbf{V}(J)$ in this case. In the exercises, you will describe an algorithm for determining whether $\overline{\mathbf{V}(I_l) \setminus \mathbf{V}(J)} = \mathbf{V}(I_l)$.

When $\mathbf{V}(I_l) \setminus \mathbf{V}(J)$ fails to be Zariski dense in $\mathbf{V}(I_l)$, Proposition 4 guarantees that we can find c_i such that the ideals

$$I^{(1)} = I + \langle c_i \rangle \quad \text{and} \quad I^{(2)} = I : c_i^\infty$$

are strictly larger than I and satisfy $V = \mathbf{V}(I) = \mathbf{V}(I^{(1)}) \cup \mathbf{V}(I^{(2)})$. Then, as in the second example above, we repeat the process on the two new ideals, which means computing FindW$(I^{(1)})$ and FindW$(I^{(2)})$. By Proposition 5, the union of these varieties works for I, which explains the last line of FindW.

We say that FindW is *recursive* since it calls itself. We leave it as an exercise to show that the maximum principle from Proposition 6 implies that FindW always terminates in finitely many steps. When it does, correctness follows from the above discussion.

We end this section by using the Closure Theorem to give a precise description of the projection $\pi_l(V) \subseteq k^{n-l}$ of an affine variety $V \subseteq k^n$.

Theorem 7. *Let k be algebraically closed and let $V \subseteq k^n$ be an affine variety. Then there are affine varieties $Z_i \subseteq W_i \subseteq k^{n-l}$ for $1 \leq i \leq p$ such that*

$$\pi_l(V) = \bigcup_{i=1}^{p} (W_i \setminus Z_i).$$

Proof. We assume $V \neq \emptyset$. First let $W_1 = \mathbf{V}(I_l)$. By the Closure Theorem, there is a variety $Z_1 \subsetneq W_1$ such that $W_1 \setminus Z_1 \subseteq \pi_l(V)$. Then, back in k^n, consider the set

$$V_1 = V \cap \{(a_1, \ldots, a_n) \in k^n \mid (a_{l+1}, \ldots, a_n) \in Z_1\}.$$

One easily checks that V_1 is an affine variety (see Exercise 10), and furthermore, $V_1 \subsetneq V$ since otherwise we would have $\pi_l(V) \subseteq Z_1$, which would imply $W_1 \subseteq Z_1$ by Zariski closure. Moreover, you will check in Exercise 10 that

$$\pi_l(V) = (W_1 \setminus Z_1) \cup \pi_l(V_1). \tag{2}$$

If $V_1 = \emptyset$, then we are done. If V_1 is nonempty, let W_2 be the Zariski closure of $\pi_l(V_1)$. Applying the Closure Theorem to V_1, we get $Z_2 \subsetneq W_2$ with $W_2 \setminus Z_2 \subset \pi_l(V_1)$. Then, repeating the above construction, we get the variety

$$V_2 = V_1 \cap \{(a_1, \ldots, a_n) \in k^n \mid (a_{l+1}, \ldots, a_n) \in Z_2\}$$

such that $V_2 \subsetneq V_1$ and

$$\pi_l(V) = (W_1 \setminus Z_1) \cup (W_2 \setminus Z_2) \cup \pi_l(V_2).$$

If $V_2 = \emptyset$, we are done, and if not, we repeat this process again to obtain W_3, Z_3 and $V_3 \subsetneq V_2$. Continuing in this way, we must eventually have $V_N = \emptyset$ for some N, since otherwise we would get an infinite descending chain of varieties

$$V \supsetneq V_1 \supsetneq V_2 \supsetneq \cdots,$$

which would contradict Proposition 1 of §6. Once we have $V_N = \emptyset$, the desired formula for $\pi_l(V)$ follows easily. □

In general, a set of the form described in Theorem 7 is called *constructible*.

As a simple example of Theorem 7, consider $I = \langle xy + z - 1, y^2z^2 \rangle \subseteq \mathbb{C}[x, y, z]$ and set $V = \mathbf{V}(I) \subseteq \mathbb{C}^3$. We leave it as an exercise to show that

$$\mathbf{V}(I_1) = \mathbf{V}(z) \cup \mathbf{V}(y, z - 1) = \mathbf{V}(z) \cup \{(0, 1)\}$$

and that $W = \mathbf{V}(y,z) = \{(0,0)\}$ satisfies $\mathbf{V}(I_1) \setminus W \subseteq \pi_1(V)$. However, we also have $\pi_1(V) \subseteq \mathbf{V}(I_1)$, and since $xy + z - 1 \in I$, no point of V has vanishing y and z coordinates. It follows that $\pi_1(V) \subseteq \mathbf{V}(I_1) \setminus \{(0,0)\}$. Hence

$$\pi_1(V) = \mathbf{V}(I_1) \setminus \{(0,0)\} = (\mathbf{V}(z) \setminus \{(0,0)\}) \cup \{(0,1)\}.$$

This gives an explicit representation of $\pi_1(V)$ as a constructible set. You will work out another example of Theorem 7 in the exercises. More substantial examples can be found in SCHAUENBURG (2007), which also describes an algorithm for writing $\pi_l(V)$ as a constructible set. Another approach is described in ULLRICH (2006).

EXERCISES FOR §7

1. Prove that Theorem 3 of Chapter 3, §2 follows from Theorem 1 of this section. Hint: Show that the W from Theorem 1 satisfies $W \subsetneq \mathbf{V}(I_l)$ when $V \neq \emptyset$.
2. In the notation of Theorem 2, prove that $\bar{I} = \langle \overline{G} \rangle$ for $\bar{I} = \{\bar{f} \mid f \in I\}$.
3. Given sets A and B, prove that $A \setminus B = A \setminus (A \cap B)$.
4. In the proof of Proposition 4, prove that $I = I : c_i^\infty$ implies that $I_l = I_l : c_i^\infty$.
5. This exercise will explore some properties of irreducible components needed in the proofs of Propositions 4 and 5.
   a. Let $W_1, \ldots, W_r$ be affine varieties contained in a variety V and assume that for each $1 \leq i \leq r$, no irreducible component of V is contained in W_i. Prove that the same is true for $\bigcup_{i=1}^r W_i$. (This fact is used in the proof of Proposition 4.)
   b. Let $W_i \subseteq V_i$ be affine varieties for $i = 1, 2$ such that W_i contains no irreducible component of V_i. Prove that $W = W_1 \cup W_2$ contains no irreducible component of $V = V_1 \cup V_2$. (This fact is used in the proof of Proposition 5.)
6. Prove Proposition 6. Hint: Assume that the proposition is false for some nonempty collection of ideals $\{I_\alpha\}_{\alpha \in \mathcal{A}}$ and show that this leads to a contradiction of the ascending chain condition.
7. In this exercise we will see why it is reasonable to make the convention that the empty product is 1. Let R be a commutative ring with 1 and let $\mathcal{A}$ be a finite set such that for every $\alpha \in \mathcal{A}$, we have $r_\alpha \in R$. Then we get the product

   $$\textstyle\prod_{\alpha \in \mathcal{A}} r_\alpha.$$

   Although $\mathcal{A}$ is unordered, the product is well-defined since R is commutative.
   a. Assume $\mathcal{B}$ is finite and disjoint from $\mathcal{A}$ such that for every $\beta \in \mathcal{B}$, we have $r_\beta \in R$. Prove that

   $$\textstyle\prod_{\gamma \in \mathcal{A} \cup \mathcal{B}} r_\gamma = \big(\prod_{\alpha \in \mathcal{A}} r_\alpha\big)\big(\prod_{\beta \in \mathcal{B}} r_\beta\big).$$

   b. It is likely that the proof you gave in part (a) assumed that $\mathcal{A}$ and $\mathcal{B}$ are nonempty. Explain why $\prod_{\alpha \in \emptyset} r_\alpha = 1$ makes the above formula work in all cases.
   c. In a similar way, define $\sum_{\alpha \in \mathcal{A}} r_\alpha$ and explain why $\sum_{\alpha \in \emptyset} r_\alpha = 0$ is needed to make the analog of part (a) true for sums.
8. The goal of this exercise is to describe an algorithm for deciding whether $\overline{\mathbf{V}(I) \setminus \mathbf{V}(g)} = \mathbf{V}(I)$ when the field k is algebraically closed.
   a. Prove that $\overline{\mathbf{V}(I) \setminus \mathbf{V}(g)} = \mathbf{V}(I)$ is equivalent to $I : g^\infty \subseteq \sqrt{I}$. Hint: Use the Nullstellensatz and Theorem 10 of §4. Also remember that $I \subseteq I : g^\infty$.
   b. Use Theorem 14 of §4 and the Radical Membership Algorithm from §2 to describe an algorithm for deciding whether $I : g^\infty \subseteq \sqrt{I}$.

9. Give a proof of the termination of FindW that uses the maximum principle stated in Proposition 6. Hint: Consider the set of all ideals in $k[\mathbf{x}, \mathbf{y}]$ for which FindW does not terminate.
10. This exercise is concerned with the proof of Theorem 7.
    a. Verify that $V_1 = V \cap \{(a_1, \ldots, a_n) \in k^n \mid (a_{l+1}, \ldots, a_n) \in Z_1\}$ is an affine variety.
    b. Verify that $\pi_l(V) = (W_1 \setminus Z_1) \cup \pi_l(V_1)$.
11. As in the text, let $V = \mathbf{V}(I)$ for $I = \langle xy + z - 1, y^2z^2\rangle \subseteq \mathbb{C}[x, y, z]$. Show that

$$\mathbf{V}(I_1) = \mathbf{V}(z) \cup \mathbf{V}(y, z - 1) = \mathbf{V}(z) \cup \{(0, 1)\}$$

    and that $W = \mathbf{V}(y, z) = \{(0, 0)\}$ satisfies $\mathbf{V}(I_1) \setminus W \subseteq \pi_1(V)$.
12. Let $V = \mathbf{V}(y - xz) \subseteq \mathbb{C}^3$. Theorem 7 tells us that $\pi_1(V) \subseteq \mathbb{C}^2$ is a constructible set. Find an explicit decomposition of $\pi_1(V)$ of the form given by Theorem 7. Hint: Your answer will involve W_1, Z_1 and W_2.
13. Proposition 6 is the maximum principle for ideals. The geometric analog is the *minimum principle* for varieties, which states that among any nonempty collection of varieties in k^n, there is a variety in the collection which is minimal with respect to inclusion. More precisely, this means that if we are given varieties V_α, $\alpha \in \mathcal{A}$, where $\mathcal{A}$ is a nonempty set, then there is some $\alpha_0 \in \mathcal{A}$ with the property that for all $\beta \in \mathcal{A}$, $V_\beta \subseteq V_{\alpha_0}$ implies $V_\beta = V_{\alpha_0}$. Prove the minimum principle. Hint: Use Proposition 1 of §6.
14. Apply the minimum principle of Exercise 13 to give a different proof of Theorem 7. Hint: Consider the collection of all varieties $V \subseteq k^n$ for which $\pi_l(V)$ is not constructible. By the minimum principle, there is a variety V such that $\pi_l(V)$ is not constructible but $\pi_l(W)$ is constructible for every variety $W \subsetneq V$. Show how the proof of Theorem 7 up to (2) can be used to obtain a contradiction and thereby prove the theorem.

§8 Primary Decomposition of Ideals

In view of the decomposition theorem proved in §6 for radical ideals, it is natural to ask whether an arbitrary ideal I (not necessarily radical) can be represented as an intersection of simpler ideals. In this section, we will prove the Lasker-Noether decomposition theorem, which describes the structure of I in detail.

There is no hope of writing an arbitrary ideal I as an intersection of prime ideals (since an intersection of prime ideals is always radical). The next thing that suggests itself is to write I as an intersection of powers of prime ideals. This does not quite work either: consider the ideal $I = \langle x, y^2\rangle$ in $\mathbb{C}[x, y]$. Any prime ideal containing I must contain x and y and, hence, must equal $\langle x, y\rangle$ (since $\langle x, y\rangle$ is maximal). Thus, if I were to be an intersection of powers of prime ideals, it would have to be a power of $\langle x, y\rangle$ (see Exercise 1 for the details).

The concept we need is a bit more subtle.

Definition 1. An ideal I in $k[x_1, \ldots, x_n]$ is **primary** if $fg \in I$ implies either $f \in I$ or some power $g^m \in I$ for some $m > 0$.

It is easy to see that prime ideals are primary. Also, you can check that the ideal $I = \langle x, y^2\rangle$ discussed above is primary (see Exercise 1).

Lemma 2. *If I is a primary ideal, then $\sqrt{I}$ is prime and is the smallest prime ideal containing I.*

Proof. See Exercise 2. □

In view of this lemma, we make the following definition.

Definition 3. If I is primary and $\sqrt{I} = P$, then we say that I is P**-primary**.

We can now prove that every ideal is an intersection of primary ideals.

Theorem 4. *Every ideal $I \subseteq k[x_1, \dots, x_n]$ can be written as a finite intersection of primary ideals.*

Proof. We first define an ideal I to be *irreducible* if $I = I_1 \cap I_2$ implies that $I = I_1$ or $I = I_2$. We claim that every ideal is an intersection of finitely many irreducible ideals. The argument is an "ideal" version of the proof of Theorem 2 from §6. One uses the ACC rather than the DCC—we leave the details as an exercise.

Next we claim that an irreducible ideal is primary. Note that this will prove the theorem. To see why the claim is true, suppose that I is irreducible and that $fg \in I$ with $f \notin I$. We need to prove that some power of g lies in I. Consider the saturation $I : g^\infty$. By Proposition 9 of §4, we know that $I : g^\infty = I : g^N$ once N is sufficiently large. We will leave it as an exercise to show that $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. Since I is irreducible, it follows that $I = I + \langle g^N \rangle$ or $I = I + \langle f \rangle$. The latter cannot occur since $f \notin I$, so that $I = I + \langle g^N \rangle$. This proves that $g^N \in I$. □

As in the case of varieties, we can define what it means for a decomposition to be minimal.

Definition 5. A **primary decomposition** of an ideal I is an expression of I as an intersection of primary ideals: $I = \bigcap_{i=1}^r Q_i$. It is called **minimal** or **irredundant** if the $\sqrt{Q_i}$ are all distinct and $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$.

To prove the existence of a minimal decomposition, we will need the following lemma, the proof of which we leave as an exercise.

Lemma 6. *If I, J are primary and $\sqrt{I} = \sqrt{J}$, then $I \cap J$ is primary.*

We can now prove the first part of the Lasker-Noether decomposition theorem.

Theorem 7 (Lasker-Noether). *Every ideal $I \subseteq k[x_1, \dots, x_n]$ has a minimal primary decomposition.*

Proof. By Theorem 4, we know that there is a primary decomposition $I = \bigcap_{i=1}^r Q_i$. Suppose that Q_i and Q_j have the same radical for some $i \neq j$. Then, by Lemma 6, $Q = Q_i \cap Q_j$ is primary, so that in the decomposition of I, we can replace Q_i and Q_j by the single ideal Q. Continuing in this way, eventually all of the Q_i's will have distinct radicals.

Next, suppose that some Q_i contains $\bigcap_{j \neq i} Q_j$. Then we can omit Q_i, and I will be the intersection of the remaining Q_j's for $j \neq i$. Continuing in this way, we can reduce to the case where $Q_i \not\supseteq \bigcap_{j \neq i} Q_j$ for all i. □

Unlike the case of varieties (or radical ideals), a minimal primary decomposition need not be unique. In the exercises, you will verify that the ideal $\langle x^2, xy\rangle \subseteq k[x, y]$ has the two distinct minimal decompositions

$$\langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, xy, y^2\rangle = \langle x\rangle \cap \langle x^2, y\rangle.$$

Although $\langle x^2, xy, y^2\rangle$ and $\langle x^2, y\rangle$ are distinct, note that they have the same radical. To prove that this happens in general, we will use ideal quotients from §4. We start by computing some ideal quotients of a primary ideal.

Lemma 8. *If I is primary with $\sqrt{I} = P$ and $f \in k[x_1, \ldots, x_n]$, then:*
(i) *If $f \in I$, then $I : f = \langle 1\rangle$.*
(ii) *If $f \notin I$, then $I : f$ is P-primary.*
(iii) *If $f \notin P$, then $I : f = I$.*

Proof. See Exercise 7. □

The second part of the Lasker-Noether theorem tells us that the *radicals* of the ideals in a minimal decomposition are uniquely determined.

Theorem 9 (Lasker-Noether). *Let $I = \bigcap_{i=1}^r Q_i$ be a minimal primary decomposition of a proper ideal $I \subseteq k[x_1, \ldots, x_n]$ and let $P_i = \sqrt{Q_i}$. Then the P_i are precisely the proper prime ideals occurring in the set $\{\sqrt{I : f} \mid f \in k[x_1, \ldots, x_n]\}$.*

Remark. In particular, the P_i are independent of the primary decomposition of I. We say that the P_i *belong* to I.

Proof. The proof is very similar to the proof of Theorem 7 from §6. The details are covered in Exercises 8–10. □

In §6, we proved a decomposition theorem for radical ideals over an algebraically closed field. Using the Lasker–Noether theorems, we can now show that these results hold over an arbitrary field k.

Corollary 10. *Let $I = \bigcap_{i=1}^r Q_i$ be a minimal primary decomposition of a proper radical ideal $I \subseteq k[x_1, \ldots, x_n]$. Then the Q_i are prime and are precisely the proper prime ideals occurring in the set $\{I : f \mid f \in k[x_1, \ldots, x_n]\}$.*

Proof. See Exercise 12. □

The two Lasker–Noether theorems do not tell the full story of a minimal primary decomposition $I = \bigcap_{i=1}^r Q_i$. For example, if P_i is minimal in the sense that no P_j is strictly contained in P_i, then one can show that Q_i is uniquely determined. Thus there is a uniqueness theorem for *some* of the Q_i's [see Chapter 4 of ATIYAH and MACDONALD (1969) for the details]. We should also mention that the conclusion of Theorem 9 can be strengthened: one can show that the P_i's are precisely the proper prime ideals in the set $\{I : f \mid f \in k[x_1, \ldots, x_n]\}$ [see Chapter 7 of ATIYAH and MACDONALD (1969)].

Finally, it is natural to ask if a primary decomposition can be done constructively. More precisely, given $I = \langle f_1, \ldots, f_s \rangle$, we can ask the following:

- (Primary Decomposition) Is there an algorithm for finding bases for the primary ideals Q_i in a minimal primary decomposition of I?
- (Associated Primes) Can we find bases for the associated primes $P_i = \sqrt{Q_i}$?

If you look in the references given at the end of §6, you will see that the answer to these questions is *yes*. Primary decomposition has been implemented in CoCoA, Macaulay2, Singular, and Maple.

EXERCISES FOR §9

1. Consider the ideal $I = \langle x, y^2 \rangle \subseteq \mathbb{C}[x, y]$.
   a. Prove that $\langle x, y \rangle^2 \subsetneq I \subsetneq \langle x, y \rangle$, and conclude that I is not a prime power.
   b. Prove that I is primary.
2. Prove Lemma 2.
3. This exercise is concerned with the proof of Theorem 4. Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal.
   a. Using the hints given in the text, prove that I is a finite intersection of irreducible ideals.
   b. Suppose that $fg \in I$ and $I : g^\infty = I : g^N$. Then prove that $(I + \langle g^N \rangle) \cap (I + \langle f \rangle) = I$. Hint: Elements of $(I + \langle g^N \rangle) \cap (I + \langle f \rangle)$ can be written as $a + bg^N = c + df$, where $a, c \in I$ and $b, d \in k[x_1, \ldots, x_n]$. Now multiply through by g and use $I : g^N = I : g^{N+1}$.
4. In the proof of Theorem 4, we showed that every irreducible ideal is primary. Surprisingly, the converse is false. Let I be the ideal $\langle x^2, xy, y^2 \rangle \subseteq k[x, y]$.
   a. Show that I is primary.
   b. Show that $I = \langle x^2, y \rangle \cap \langle x, y^2 \rangle$ and conclude that I is not irreducible.
5. Prove Lemma 6. Hint: Proposition 16 from §3 will be useful.
6. Let I be the ideal $\langle x^2, xy \rangle \subseteq \mathbb{Q}[x, y]$.
   a. Prove that
   $$I = \langle x \rangle \cap \langle x^2, xy, y^2 \rangle = \langle x \rangle \cap \langle x^2, y \rangle$$
   are two distinct minimal primary decompositions of I.
   b. Prove that for any $a \in \mathbb{Q}$,
   $$I = \langle x \rangle \cap \langle x^2, y - ax \rangle$$
   is a minimal primary decomposition of I. Thus I has infinitely many distinct minimal primary decompositions.
7. Prove Lemma 8.
8. Prove that an ideal is proper if and only if its radical is.
9. Use Exercise 8 to show that the primes belonging to a proper ideal are also proper.
10. Prove Theorem 9. Hint: Adapt the proof of Theorem 7 from §6. The extra ingredient is that you will need to take radicals. Proposition 16 from §3 will be useful. You will also need to use Exercise 9 and Lemma 8.
11. Let $P_1, \ldots, P_r$ be the prime ideals belonging to I.
   a. Prove that $\sqrt{I} = \bigcap_{i=1}^r P_i$. Hint: Use Proposition 16 from §3.
   b. Show that $\sqrt{I} = \bigcap_{i=1}^r P_i$ need not be a minimal decomposition of $\sqrt{I}$. Hint: Exercise 4.
12. Prove Corollary 10. Hint: Use Proposition 9 of §4 to show that $I : f$ is radical.

§9 Summary

The table on the next page summarizes the results of this chapter. In the table, it is supposed that all ideals are radical and that the field is algebraically closed.

ALGEBRA		GEOMETRY
radical ideals		varieties
I	$\longrightarrow$	$\mathbf{V}(I)$
$\mathbf{I}(V)$	$\longleftarrow$	V
addition of ideals		intersection of varieties
$I+J$	$\longrightarrow$	$\mathbf{V}(I)\cap\mathbf{V}(J)$
$\sqrt{\mathbf{I}(V)+\mathbf{I}(W)}$	$\longleftarrow$	$V\cap W$
product of ideals		union of varieties
IJ	$\longrightarrow$	$\mathbf{V}(I)\cup\mathbf{V}(J)$
$\sqrt{\mathbf{I}(V)\mathbf{I}(W)}$	$\longleftarrow$	$V\cup W$
intersection of ideals		union of varieties
$I\cap J$	$\longrightarrow$	$\mathbf{V}(I)\cup\mathbf{V}(J)$
$\mathbf{I}(V)\cap\mathbf{I}(W)$	$\longleftarrow$	$V\cup W$
ideal quotients		difference of varieties
$I:J$	$\longrightarrow$	$\overline{\mathbf{V}(I)\setminus\mathbf{V}(J)}$
$\mathbf{I}(V):\mathbf{I}(W)$	$\longleftarrow$	$\overline{V\setminus W}$
elimination of variables		projection of varieties
$I\cap k[x_{l+1},\ldots,x_n]$	$\longleftrightarrow$	$\overline{\pi_l(\mathbf{V}(I))}$
prime ideal	$\longleftrightarrow$	irreducible variety
minimal decomposition		minimal decomposition
$I=P_1\cap\cdots\cap P_m$	$\longrightarrow$	$\mathbf{V}(I)=\mathbf{V}(P_1)\cup\cdots\cup\mathbf{V}(P_m)$
$\mathbf{I}(V)=\mathbf{I}(V_1)\cap\cdots\cap\mathbf{I}(V_m)$	$\longleftarrow$	$V=V_1\cup\cdots\cup V_m$
maximal ideal	$\longleftrightarrow$	point of affine space
ascending chain condition	$\longleftrightarrow$	descending chain condition